1 Дјељивост, НЗД...

1

Ако је $a = qb + r$, доказати да вриједи да нзд$(a, b) =$ нзд(b, r)

Доказ. Нека је $d =$ нзд$(a, a + n)$. Како d дијели... □

(**Марко Симоновић 10/18 Д**) задатак преузетса
`https://math.vanderbilt.edu/rolenl/IntroNTExam1S.pdf`

2

Доказати да за природан број n и цио број a, вриједи да нзд$(a, a+n)$ дијели n.

Доказ. Нека је $d =$ нзд$(a, a + n)$. Како d дијели... □

(**Павле Радојевић 14/17 Д**) задатак преузет из књиге Exercises in Number theory:
`https://link.springer.com/book/10.1007/978-1-4757-5194-9`

3

(а) Нека је нзд$(a, b) = 1$. Ако $b \mid c$ и $a \mid c \Rightarrow ab \mid c$.
(б) Ако су a и b позитивни цијели бројеви, доказати да (a, b) дијели $a + b$ и $[a, b]$.

Доказ. (а) $\exists x, y \in \mathbb{Z}$ тако да $1 = ax + by$. Па, $c = acx + bcy$. Како су оба елемента са десне стране дјељива са ab, онда такође имамо да $ab \mid c$.

(б) Из дефиниције можемо рећи да $d = (a, b)$ дијели и a и b, па ћемо записати $a = kd$ и $b = md$ за цијеле бројеве k и m. Онда, $a+b = kd+md = d(k+m)$, па d дијели $a+b$ како је и тражено. Затим, по дефиницији имамо да a дијели $[a, b]$, па то можемо записати на следећи

начин $[a,b] = pa$, за неки цијели број p. Али онда имамо да $[a,b] = pa = p(kd) = d(kp)$, па d дијели $[a,b]$, што је и тражено.

□

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://www.math.pitt.edu/~sparling/081/10281/10281quizzes/10281e2s.pdf\https://www.a-eskwadraat.nl/Onderwijs/Boekweb/Artikel/41/Dictaat/Downloaden`

4

(а) Одредити $d = \text{нзд}(196, 154)$ користећи Еуклидов алгоритам и написати d као линеарну комбинацију 196 и 154.
(б) Одредити $\text{нзд}(75, 625, 1050, 1400)$ примјеном Еуклидовог алгоритма.

Доказ. (а)

$$\begin{aligned} 196 &= 154 \cdot 1 + 42 \\ 154 &= 42 \cdot 3 + 28 \\ 42 &= 28 \cdot 1 + 14 \\ 28 &= 14 \cdot 2 \end{aligned}$$

Добили смо да је $d = \text{нзд}(196, 154) = 14$. Сада број 14 можемо представити као линерану комбинацију.

$$\begin{aligned} 14 &= 42 - 28 \cdot 1 \\ &= 42 - (154 - 42 \cdot 3) \cdot 1 \\ &= 4 \cdot 42 - 1 \cdot 154 \\ &= 4 \cdot (196 - 154 \cdot 1) - 1 \cdot 154 \\ &= 4 \cdot 196 - 5 \cdot 154 \\ &= 196 \cdot 4 + 154 \cdot (-5) \end{aligned}$$

(б) Имамо $\text{нзд}(75, 625, 1050, 1400) = \text{нзд}(\text{нзд}(75, 625, 1050), 1400) = \text{нзд}(\text{нзд}(\text{нзд}(75, 625), 1050), 1400)$.
Прво тражимо $\text{нзд}(75, 625)$.

$$\begin{aligned} 625 &= 8 \cdot 75 + 25 \\ 75 &= 3 \cdot 25 \end{aligned}$$

Дакле, $\text{нзд}(75, 625) = 25$, па се тражена једнакост своди на:
$\text{нзд}(75, 625, 1050, 1400) = \text{нзд}(\text{нзд}(25, 1050), 1400)$
Сада тражимо $\text{нзд}(25, 1050)$.

$$1050 = 42 \cdot 25$$

Дакле, нзд$(25, 1050) = 25$, па се полазна једнакост сада своди на:
нзд$(75, 625, 1050, 1400) =$ нзд$(25, 1400)$

$$1400 = 56 \cdot 25$$

Добили смо да је нзд$(75, 625, 1050, 1400) = 25$. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://elib.mi.sanu.ac.rs/files/journals/nm/245/nm581202.pdf`
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

5

Нека је нзд$(a, b) = 1$. Доказати:
(а) нзд$(a + b, a - b) = 1 \vee 2$
(б) нзд$(2a + b, a + 2b) = 1 \vee 3$

Доказ. (а) Нека је $d =$ нзд$(a + b, a - b)$, гдје је d дјелиац свих линеарних комбинација од $a + b$ и $a - b$. Дакле,

$$d \mid (a + b) + (a - b) \Rightarrow d \mid 2a$$

и имамо следеће:

$$d \mid (a + b) - (a - b) \Rightarrow d \mid 2b.$$

Даље имамо да је $d \leq$ нзд$(2a, 2b) = 2\,$нзд$(a, b) = 2 \Rightarrow d = 1 \vee 2$, што је и требало доказати.

(б) Нека је $d =$ нзд$(2a + b, a + 2b)$, па као и у претходном примјеру, d је дјелилац свих линераних комбинација од $2a + b$ и $a + 2b$ и на основу тога пишемо

$$d \mid 2(2a + b) - (a + 2b) \iff d \mid 3a$$

и имамо следеће:

$$d \mid -1(2a + b) + 2(a + 2b) \iff d \mid 3b.$$

Слиједи

$$d \leq \text{нзд}(3a, 3b) = 3\,\text{нзд}(a, b) = 3,$$

па је $d = 1, 2 \vee 3$. Ако је $d = 2$, онда из нзд$(2, 3) = 1$ и **Еуклидове леме** слиједи да $d \mid 3a \Rightarrow d \mid a$ и $d \mid 3b \Rightarrow d \mid b$. Међутим, ако $2 \mid a$ и $2 \mid b$, онда је нзд$(a, b) \neq 1$, па је $d \neq 2$ и на тај начин добијамо оно што је тражено, тј. да је $d = 1 \vee 3$.

Еуклидова лема: Нека је p прост број и нека су a и b цијели бројеви, такви да $p \mid a \cdot b$, тада $p \mid a$ или $p \mid b$. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
http://www.americanriver.com/files/burton_elementary_number_theory/02-3%20The%20Euclidean%20Algorithm.pdf

6

Нека су a и b природни бројеви, такви да је $a < b$. Доказати да се међу произвољних b узастопних природних бројева могу наћи два чији је производ дјељив са ab.

Доказ. Нека је $\{x_1, x_2 \dots x_b\}$ скуп од b узастопних природних бројева. Тада се међу њима налази број x_i дјељив са b и због $a < b$, број x_j дјељив са a. Претпоставимо да је $i = j$. Означимо са d највећи заједнички дјелилац бројева a и b, а са s њихов најмањи заједнички садржалац. Тада је $ds = ab$ и $s \mid x_i$. Докажимо да бар један од бројева $x_i + d$ и $x_i - d$ (који су дјељиви са d) припада скупу $\{x_1, x_2 \dots x_b\}$.

Ако то не би био случај, било би $x_i + d > x_b$ и $x_i - d < x_1$, одакле би слиједило $2d > x_b - x_1 + 1 = b$. Међутим, због $d \mid b$, то би значило да је $d = b > a$, па не би могло да важи $d \mid a$, што је супротно дефиницији броја d.
Ако $x_i + d \in \{x_1, x_2 \dots x_b\}$, тада је производ $x_i(x_i + d)$ дјељив са $ds = ab$, а у супротном је $x_i(x_i - d)$ дјељиво са ab, чиме је доказ завршен.

□

(**Катарина Синђић 36/19 Д**) задатак преузет са https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf

7

Доказати да је $mn(m^4 - n^4)$ дјељив са 30 за сваки природан број m и n.

Доказ. Раставићемо дати израз, $mn(m^4 - n^4) = n(m^5 - m) + m(n - n^5)$. Доказаћемо да $30 \mid n(m^5 - m)$ и $30 \mid m(n - n^5)$. Када то докажемо, добићемо директно да $30 \mid mn(m^4 - n^4)$. Кренимо са доказивањем.

(1)Доказаћемо да $30 \mid n(m^5 - m)$.

$$\begin{aligned} n(m^5 - m) &= nm(m^4 - 1) \\ &= nm(m^2 - 1)(m^2 + 1) \\ &= nm(m - 1)(m + 1)(m^2 + 1), \end{aligned}$$

где су $(m - 1)m(m + 1)$ три узастопна броја. $\Longrightarrow$

$$\begin{aligned} 2 \mid (m - 1)m(m + 1) \\ 3 \mid (m - 1)m(m + 1). \end{aligned}$$

Како бројеви 2 и 3 дијеле три узастопна броја, онда и број 6 дијели три узастопна броја, односно

$$\begin{aligned} &6 \mid (m-1)m(m+1) \\ \implies\ &6 \mid n(m^5-m). \end{aligned}$$

Сада треба да докажемо да $5 \mid n(m^5-m)$. То ћемо радити на следећи начин:

$$\begin{aligned} &m = 5k \implies (m-1)m(m+1) = (5k-1)5k(5k+1) \\ &\implies 5 \mid (m-1)m(m+1) \\ &\implies 5 \mid n(m^5-m). \end{aligned}$$

$$\begin{aligned} &m = 5k+1 \implies (m-1)m(m+1) = 5k(5k+1)(5k+2) \\ &\implies 5 \mid (m-1)m(m+1) \\ &\implies 5 \mid n(m^5-m). \end{aligned}$$

$$\begin{aligned} &m = 5k+2 \implies (m^2+1) = (5k+2)^2+1 \\ &= 25k^2+20k+5 \\ &= 5(5k^2+4k+1) \\ &\implies 5 \mid n(m^5-m). \end{aligned}$$

$$\begin{aligned} &m = 5k+3 \implies (m^2+1) = (5k+3)^2+1 \\ &= 25k^2+30k+10 \\ &= 5(5k^2+6k+2) \\ &\implies 5 \mid n(m^5-m). \end{aligned}$$

Из $m = 5k, 5k+1, 5k+2, 5k+3$ добијамо да $5 \mid n(m^5-m)$. Па, како

$$6 \mid n(m^5-m) \wedge 5 \mid n(m^5-m),$$

добијамо да $30 \mid n(m^5-m)$.
Сада ћемо на исти начин да докажемо да $30 \mid m(n-n^5)$.

(2)Доказаћемо да $30 \mid m(n-n^5)$.

$$\begin{aligned} m(n-n^5) &= mn(1-n^4) \\ &= -mn(n^4-1) \\ &= -mn(n^2-1)(n^2+1) \\ &= -mn(n-1)(n+1)(n^2+1), \end{aligned}$$

где су $(n-1)n(n+1)$ три узастопна броја. $\implies$

$$\begin{aligned} &2 \mid (n-1)n(n+1) \\ &3 \mid (n-1)n(n+1). \end{aligned}$$

Како бројеви 2 и 3 дијеле три узастопна броја, онда и број 6 дијели три узастопна броја, односно

$$\begin{aligned} &6 \mid (n-1)n(n+1) \\ \implies\ &6 \mid m(n-n^5). \end{aligned}$$

Сада треба да докажемо да $5 \mid m(n-n^5)$. То ћемо радити на следећи начин:

$$\begin{aligned} &n = 5k \implies (n-1)n(n+1) = (5k-1)5k(5k+1) \\ &\implies 5 \mid (n-1)n(n+1) \\ &\implies 5 \mid m(n-n^5). \end{aligned}$$

$$\begin{aligned} &n = 5k+1 \implies (n-1)n(n+1) = 5k(5k+1)(5k+2) \\ &\implies 5 \mid (n-1)n(n+1) \\ &\implies 5 \mid m(n-n^5). \end{aligned}$$

$$\begin{aligned} &n = 5k+2 \implies (n^2+1) = (5k+2)^2+1 \\ &= 25k^2+20k+5 \\ &= 5(5k^2+4k+1) \\ &\implies 5 \mid m(n-n^5). \end{aligned}$$

$$\begin{aligned} &n = 5k+3 \implies (n^2+1) = (5k+3)^2+1 \\ &= 25k^2+30k+10 \\ &= 5(5k^2+6k+2) \\ &\implies 5 \mid m(n-n^5). \end{aligned}$$

Из $n = 5k, 5k+1, 5k+2, 5k+3$ добијамо да $5 \mid m(n-n^5)$. Па, како

$$6 \mid m(n-n^5) \wedge 5 \mid m(n-n^5),$$

добијамо да $30 \mid m(n-n^5)$. Из (1) и (2) смо добили да

$$30 \mid n(m^5-m) \wedge 30 \mid m(n-n^5),$$

што значи да $30 \mid mn(m^4-n^4)$. Тиме је доказ завршен. □

(**Катарина Синђић 36/19 Д**) задатак преузет са домаћег из предмета Математика 5.

8

За произвољан природан број a и цијели број b постоје јединствени цијели бројеви q и r такви да је $b = qa + r, 0 \leq r < a$.

Доказ. Посматрајмо скуп $b - am : m \in Z$.Најмањи ненегативан члан овог скупа означимо са r. Тада је по дефиницији $0 \leq r < a$ и постоји $q \in Z$ $b - qa = r$, такав да је $b = qa + p$, тј. $b = qa + r$. Да би доказали јединственост од q и r, претпоставимо да постоји још један пар q_1, r_1 који задовољава исте захтјеве. Покажимо најприје да је $r_1 = r$. Претпоставимо да је нпр. $r < r_1$. Тада је $0 < r_1 - r < a$, док је с друге стране $r_1 - r = a(q - q_1) \leq a$. Према томе је $r_1 = r$, па је стога и $q_1 = q$.

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`https://www.academia.edu/2991414/Uvod_u_teoriju_brojeva_skripta_`

9

Одредити НЗД(75, 625, 1050, 1400).

Доказ. Применом Еуклидовог алгоритма као у теореми решавамо задатак:

$$\begin{aligned} \text{нзд}(75, 625, 1050, 1400) &= \text{нзд}(\text{нзд}(75, 625, 1050), 1400) \\ &= \text{нзд}(\text{нзд}(\text{нзд}(75, 625), 1050), 1400) \end{aligned}$$

Прво тражимо нзд$(75, 625)$:

$$\begin{aligned} 625 &= 8 \cdot 75 + 25 \\ 75 &= 3 \cdot 25 \end{aligned}$$

Дакле нзд$(75, 625) = 25$, па се тражена једнакост своди на:

$$\text{нзд}(75, 625, 1050, 1400) = \text{нзд}(\text{нзд}(25, 1050), 1400)$$

Сада тражимо НЗД(25, 1050):

$$1050 = 42 \cdot 25$$

Дакле нзд$(25, 1050) = 25$, па се полазна једнакост своди сада на:

$$\begin{aligned} \text{нзд}(75, 625, 1050, 1400) &= \text{нзд}(25, 1400) \\ 1400 &= 56 \cdot 25 \\ \text{нзд}(75, 625, 1050, 1400) &= 25. \end{aligned}$$

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

10

Одредити $d = \text{нзд}\,(936, 588)$ користећи Еуклидов алгоритам.

Доказ. Према Еуклидовом алгоритму имамо следећи низ:

$$\begin{aligned} 936 &= 1 \cdot 588 + 348, \\ 588 &= 1 \cdot 348 + 240, \\ 348 &= 1 \cdot 240 + 108, \\ 240 &= 2 \cdot 108 + 24, \\ 108 &= 4 \cdot 24 + 12, \\ 24 &= 2 \cdot 12. \end{aligned}$$

Дакле, (936,588) = 12.
Вратимо се поново Еуклидовом алгоритму и напишимо остатке на следећи начин:

$$\begin{aligned} r_1 &= a - q_1 b, \\ r_2 &= b - q_2 r_1, \\ r_3 &= r_1 - q_3 r_2, \\ &\ldots \\ r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2}, \\ r_k &= r_{k-2} - q_k r_{k-1}. \end{aligned}$$

Видимо да се у овом низу, почев од трећег, сваки члан изражава помоћу своја два претходника као целобројна линеарна комбинација. Ако сада пођемо од последњег члана r_k у наведеном низу, закључујемо да се он може изразити као линеарна комбинација бројева a и b са целобројним коефицијентима:

$$r_k = ax + by; \quad x, y \in Z.$$

Тиме смо доказали да ако су a и b цијели бројеви, једначина $\mathbf{ax + by = (a,b)}$ има бар једно цјелобројно рјешење. □

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://operator.pmf.ni.ac.rs/www/pmf/publikacije/Mii/2008-2009/broj%201%20sveska%201-2/mii1-4.pdf`

11

Ако су a и b решења једначине $x^2+px-1=0$, гдје је p непаран број, тада су, за сваки ненегативан цео број n, бројеви a^n+b^n и $a^{n+1}+b^{n+1}$ цијели и узајамно прости. Доказати.

Доказ. Према Виетовим формулама је $a+b=-p$ и $ab=-1$. Доказаћемо тврђење задатка индукцијом.
За $n=0$ имамо да су $a^0+b^0=2$ и $a^1+b^1=-p$ узајамно прости. Нека су a^n+b^n и $a^{n+1}+b^{n+1}$ цијели и узајамно прости бројеви. Број

$$\begin{aligned} a^{n+2}+b^{n+2} &= (a+b)(a^{n+1}+b^{n+1})-ab(a^n+b^n) \\ &= -p(a^{n+1}+b^{n+1})+(a^n+b^n) \end{aligned}$$

је такође цео. Ако бројеви $a^{n+2}+b^{n+2}$ и $a^{n+1}+b^{n+1}$ не би били узајамно прости, тада не би били узајамно прости ни бројеви $a^{n+1}+b^{n+1}$ и a^n+b^n. Одатле слиједи тврђење задатака. □

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

12

Нека је p прост број и нека су a и b цијели бројеви такви да $p \mid a \cdots b$. Тада $p \mid a$ или $p \mid b$.

Доказ. Нека p не дијели једног од бројева a,b. Можемо претпоставити да p ł a. Требамо доказати да тада p дијели b. Како p не дијели цијели број a, а једини дјелитељи простог броја p су 1 и p, слиједи да је (a,p) = 1. Постоје цијели бројеви x, y такви да је $ax+py=1$. Множењем с b добијамо $abx+pby=b$. Како p дијели b, слиједи да p дијели b, што је и требало доказати.

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`https://www.mathos.unios.hr/~imatic/uvod%20u%20teoriju%20brojeva.pdf`

13

Доказати да за сваки природан број n важи:
(1) $6|n^3+5n$; (2) $30|n^5-n$; (3) $120|n^5-5n^3+4n$.

Доказ. Ова тврђења се доказују применом принципа математичке индукције , али да она важе може се видети из одговарајућих једнакости.
(1) $n^3+5n = n^3-n+6n = (n-1)n(n+1)+6n$.
Како $2|(n-1)n(n+1)$, $3|(n-1)n(n+1)$ и $(2,3)=1$,то важи
$2\cdot 3 = 6|(n-1)n(n+1)$.

(2) $n^5-n = n(n^4-1) = (n-1)n(n+1)(n^2+1)$.
Према (1)$6|(n-1)n(n+1)$. Могуће је да наступе следећи случајеви:

(i) $n = 5k$, за неки број к$\in Z$;

(ii) $n = 5k+1$, за неки број к$\in Z$, тада је $n-1 = 5k$;

(iii) $n = 5k+2$, за неки број к$\in Z$, тада је $n^2+1 = 5(5k^2+2k+1)$;

(iv) $n = 5k+3$, за неки број к $\in Z$, тада је $n^2+1 = 5(5k^2+6k+2)$;

(v) $n = 5k+4$, за неки број к $\in Z$, тада је $n+1 = 5(k+1)$

$$(3)\quad n^5-5n^3+4n = n(n^4-5n^2+4) = n(n^2-4)(n^2-1)$$
$$=(n-2)(n-1)n(n+1)(n+2).$$

Производ пет узастопних бројева дјељив је са **5! = 120**.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

14

Колико има природних бројева који нису већи од 2 004 за које важи $[\sqrt{n}]\,|n$?

Доказ. Нека је $[\sqrt{n}] = k$. Тада је

$k \le \sqrt{n} < k+1$ тј. $k^2 \le n < k^2+2k+1$.

Између узастопних квадрата k^2 и $(k+1)^2$ само су бројеви k^2, k^2+k и k^2+2k дјељиви са k . Према томе, у сваком од интервала $\left[1^2,2^2\right), \left[2^2,3^2\right), \ldots, \left[43^2,44^2\right)$, постоје три природна броја који задовољавају дати услов. Како је $44^2 = 1936, 44^2+44 = 1980$и $44^2+2\cdot 44 = 2024$, бројева са траженом особином има $513\cdot 43+2 = 131$.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

15

Доказати да је збир $2n+1$ узастопних природних бројева дјељив са $2n+1$.

Доказ. Нека k буде почетни број. Онда $2n+1$ узастопних природних бројева можемо приказати као:

$$k,\ k+1,\ k+2,\ldots,\ k+2n$$

Тада суму ових бројева можемо приказати као:

$$S(k,n) = (2n+1)k + \tfrac{2n(2n+1)}{2} = (2n+1)(k+n)$$

Што значи да $(2n+1) \mid S(k,n)$ □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге TEORIJA BROJEVA:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

16

Пронаћи највећи позитиван цијели број n за који важи: $(n+10) \mid (n^3+100)$

Доказ. Нека је $m = n+10 \Rightarrow n = m-10$. Тада n^3+100 можемо приказати као:

$$n^3 + 100 = (m-10)^3 + 100 = m^3 - 30m^2 + 300m - 900$$

Како у поставци $(n+10) \mid (n^3+100)$, тако сада имамо да

$$m \mid (m^3 - 30m^2 - 300m - 900)$$

А како m дијели сваки од ових бројева m^3, $30m^2$, $300m \Rightarrow m \mid 900$
Највећи број m за који ово важи је сам број 900, па је $m = 900$, односно $n = m-10 = 890$ □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге 250 Problems in Elementary Number Theory:
`https://onlinelibrary.wiley.com/doi/abs/10.1002/zamm.19720520820`

17

Доказати да $42 \mid n^7 - n$ за све позитивне цијеле бројеве n.

Доказ. Уочимо да је $42 = 7 \cdot 3 \cdot 2$, што значи да треба да докажемо да:

$$2 \mid n^7 - n$$
$$3 \mid n^7 - n$$
$$7 \mid n^7 - n$$

Kako je 7 prost broj po Mala Fermaovoj teoremi možemo zaključiti da $7 \mid n^7 - n$.
Zatim, kako su i n^7 i n neparni brojevi, onda je $n^7 - n$ paran broj $\Rightarrow 2 \mid n^7 - n$
I na kraju

$$n^7 - n = n(n^6 - n) = n((n^2)^3 - 1) = n(n^2 - 1)(n^4 + n^2 + 1) = (n^3 - n)(n^4 + n^2 + 1)$$

$\Rightarrow 3 \mid n^7 - n$ čime je naš dokaz završen. □

(**Ирвин Хуремовић 19/17 Д**) zadatak preuzet iz:
`https://www.math.toronto.edu/~herzig/putnam_nt_oct07.pdf`

18

Dokazati da se za $n \in N$ razlomak $\dfrac{21n+4}{14n+3}$ ne može skratiti.

Dokaz. Da bismo dokazali da se ovaj razlomak ne može skratiti, dovoljno je da dokažemo da je $\text{nzd}(21n+4, 14n+3) = 1$
Kako je

$$-2(21n+4) + 3(14n+3) = -42n - 8 + 42n + 9 = 1$$

$\Rightarrow \text{nzd}(21n+4, 14n+3) = 1$, odnosno razlomak se ne može skratiti. □

(**Ирвин Хуремовић 19/17 Д**) zadatak preuzet iz knjige TEORIJA BROJEVA:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

19

Dokazati da ni za jedan prirodan broj n broj $1^{2005} + 2^{2005} + ... + n^{2005}$ nije djeljiv sa $n+2$.

Dokaz. Neka je k neki neparan prirodni broj. Onda $x + y \mid x^k + y^k$.
Ako zamijenimo $x = -y$, dobijamo $x^k + y^k = x^k + (-x)^k = 0$.
Označimo sada redom brojeve $1, 2, ...$ sa n pa dobijamo:

$$(m^{2005} + (n - m + 2)^{2005})$$

Jasno je da je ovaj broj djeljiv sa $m + (n - m + 2) = n + 2$. Što znači da je:

$$\begin{aligned} 2(1^{2005} + 2^{2005} + ... + n^{2005}) &= 2 + (2^{2005} + n) + (3^{2005} + (n-1)^{2005}) + ... + (n + 2^{2005}) \\ &= 2 + S_2(n+2) + S_3(n+2) + ... + S_n(n+2) \\ &= 2 + (n+2)[S_2 + ... + S_n] \\ &= 2 + (n+2)M \end{aligned}$$

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге TEORIJA BROJEVA:
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

20

Ако су a, b, c цели бројеви, $m, n, \in N$, доказати да важи:

1) $(a, c) = 1, (b, c) = 1 \Rightarrow (ab, c) = 1$;

2) $(a, b) = 1 \Rightarrow (a^m, b^n) = 1$;

3) $a \mid c,\ \ b \mid c,\ \ (a, b) = 1 \Rightarrow ab \mid\ \ c$

Доказ. 1) Како је $(a, c) = 1$, постоје бројеви $\alpha, \gamma_1 \in Z$ такви да је $\alpha a + \gamma_1 c = 1$. Слично из $(b, c) = 1$ следи да постоје бројеви $\beta, \gamma_2 \in Z$ такви да је $\beta b + \gamma_2 c = 1$. Тада је $\alpha a \beta b = (1 - \gamma_1 c)(1 - \gamma_2 c)$, односно $\alpha\beta ab + (\gamma_1 + \gamma_2 - \gamma_1\gamma_2 c)c = 1$, одакле следи да је $(ab, c) = 1$.

2) Према 1) имамо:

$$(a, b) = 1 \Rightarrow (a^2, b) = 1 \Rightarrow \cdots \Rightarrow (a^m, b) = 1$$
$$\Rightarrow (a^m, b^2) = 1 \Rightarrow \cdots \Rightarrow (a^m, b^n) = 1.$$

3) Због $(a, b) = 1$ је $[a, b] = ab$. Како $a \mid c$ и $b \mid c$ то и $[a, b] \mid c$, односно $ab \mid c$.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

21

Доказати да је за сваки природан број n бар један од бројева $3^{3n} + 2^{3n}$ и $3^{3n} - 2^{2n}$ дјељив са 35

Доказ. Ако је n непаран број , онда је $3^{3n} + 2^{3n} = 27^n + 8^n$, па $27 + 8 = 35 \mid 27^n + 8^n$. Ако је $n = 2k$, за неки број $k \in N$, онда је

$$3^{3n} - 2^{3n} = 3^{6k} - 2^{6k} = 729^k - 64^k = (729 - 64)\sum_{i=0}^{k-1} 729^{k-1-i}64^i,$$

на тврђење следи, јер је $729 - 64 = 19 \cdot 35$.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

22

Нека су a, b и c цели бројеви такви да важи $a+b+c \mid a^2+b^2+c^2$.
Доказати да постоји бесконачно много природних бројева n за које важи

$$a+b+c \mid a^n+b^n+c^n.$$

Доказ. Докажимо индукцијом по броју k да је за све природне бројеве облика $n = 2^k$ испуњено:

$$a+b+c \mid a^n+b^n+c^n, a+b+c \mid 2(a^nb^n+b^nc^n+c^na^n).$$

За $k=1$ прво тврђење је очигледно, а друго следи из

$$2(ab+bc+ca) = (a+b+c)^2 - (a^2+b^2+c^2).$$

Нека тврђење важи за неко k. Из

$$a^{2^{k+1}} + b^{2^{k+1}} + c^{2^{k+1}} = \left(a^{2^k} + b^{2^k} + c^{2^k}\right)^2 - 2\left(a^{2^k}b^{2^k} + b^{2^k}c^{2^k} + c^{2^k}a^{2^k}\right)$$

добијамо прво тврђење и за $k+1$, а из

$$a^{2^{k+1}}b^{2^{k+1}} + b^{2^{k+1}}c^{2^{k+1}} + c^{2^{k+1}}a^{2^{k+1}}$$

$$= \left(a^{2^k}b^{2^k} + b^{2^k}c^{2^k} + c^{2^k}a^{2^k}\right) - 2\left(a^{2^k} + b^{2^k} + c^{2^k}\right)a^{2^k}b^{2^k}c^{2^k}$$

и друго.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

23

Пронаћи све цијеле бројеве такве да
$x-3 \mid x^3-3$

Доказ. Нека је $x-3=t$ Онда је t цијели број $\neq 0$ такав да $t \mid (t+3)^2-3$, што одговара услову $t \mid 3^3-3$, или $t \mid 24$. Према томе, неопходно је и кључно за t да буде цијелобројни дијелилац броја 24, стога t мора бити једнако једном од бројева $\pm1, \pm2, \pm3 \pm 4, \pm6, \pm8, \pm12, \pm24$. За $x = t+3$ можемо имати следеће вриједности $-24, -9, -5, -3, -1, 0, 1, 2, 4, 5, 6, 7, 9, 11, 15$ и 27.

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

24

Доказати да за позитиван цијели број m и $a > 1$ важи

$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m)$$

Доказ. Нека је $d = \left(\frac{a^m-1}{a-1}, a - 1\right) = (a - 1, m)$. С обзиром на идентитет

$$\frac{a^m - 1}{a - 1} = (a^{m-1} - 1) + (a^{m-2} - 1) + ... + (a - 1) + m \tag{1.1}$$

и узимајући у обзир чињеницу: $a - 1 \mid a^k - 1$ за $k = 0, 1, 2, \ldots$ добијамо да је $d \mid m$. Према томе, ако бројеви $a - 1$ и m имају заједничког дијелиоца $\delta > d$, имамо, по (1.1), релацију $\delta \mid \frac{a^m-1}{a-1}$ и бројеви $\frac{a^m-1}{a-1}$ и $a-1$ ће имати заједничког дијелиоца $\delta > d$ што није могуће. Према томе d је највећи заједнички дијелилац бројева $a - 1$ и m, што је и требало доказати. □

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

25

Доказати да постоји бесконачно много позитивних цијелих бројева n таквих да $n \mid 2^n + 1$, пронаћи све такве просте бројеве

Доказ. Требамо да докажемо да ако је n парно и такво да $n \mid 2^n + 2$ и $n - 1 \mid 2^n + 1$ (што је тачно, на примјер за $n = 2$)онда за број $n_1 - 1 = 2^n + 2$, такође имамо $n_1 \mid 2^{n_1} + 2$ и $n_1 - 1 \mid 2^{n_1} + 1$. Дакле ако је $n \mid 2^n + 2$ и ако је n паран, онда је $2^n + 2 = nk$, гдје је k непаран, према томе:

$$2^n + 1 \mid 2^{nk} + 1 = 2^{n^k+2} + 1$$

и за $n_1 = 2^n + 2$ имамо

$$n_1 - 1 = 2^n + 1 \mid 2^{n_1} + 1$$

Слиједи, имамо $n - 1 \mid 2^n + 1$, што имплицира $2^n + 1 = (n - 1)m$, гдје је m непарно. Дакле имамо $2^{n-1} \mid 2^{(n-1)m} + 1$, што даље значи $2^n + 2 \mid 2^n + 2 \mid 2^{2^n+2} + 2$, или $n_1 \mid 2^{n_1} + 2$ Пошто је $n_1 = 2^n + 2 > n$, онда постоји бесконачно много парних бројева n који задовољавају услове. Почев од $n = 2$, имамо суксесивно бројеве $2, 6, 66, 2^{66} + 2, \ldots$. □

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

26

Доказати да не постоје цијели бројеви $n > 1$ за које је $n \mid 2^n - 1$

Доказ. Претпоставимо да постоје позитивни цијели бројеви $n > 1$ за које важи $n \mid 2^n - 1$, и нека n означава најмањи од њих. По Ојлеровој теореми, можемо имати $n \mid 2^{\phi(n)} - 1$. Међутим највећи заједнички дјијелилац бројева $2^a - 1$ и $2^b - 1$ за позитивне цијеле бројеве a и b је број $2^d - 1$, гдје је $d = (a, b)$. За $a = b$ и $b = \phi(n)$, $d = (n, \phi(n))$, слиједи да је $n \mid 2^d - 1$. Међиутим пошто је $n > 1$, имамо $2^d - 1$, што имплицира да је $d > 1$ и $1 < d \leq \phi(n) < n$, и $d \mid n \mid 2^d - 1$ супротно дефиницији n. □

(**Љиљана Госпић 2/17 Д**) задатак преузет са
https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf

27

За сваки позитиван цијели број a, пронаћи композитни број n такав да $n \mid a^n - a$

Доказ. Ако је a композитно, можемо поставити да је $n = a$ због очигледног $a \mid a^n - a$. Ако је $a = 1$ можемо поставити да је $n = 4$ због $4 \mid 1^4 - 1$.Ако је a прост број > 2, можемо поставити $n = 2a$, и у том случају a је непаран број, а број $a^{2a} - a$ је паран; по томе, је $a^{2a} - a$ дијељиво са непарним бројем a и са 2, па је дијељив је и са $2a$.
Остаје нам да размотримо случај када је $a = 2$. Овдје можемо поставити да је $n = 341 = 11 \cdot 31$, јер је $341 \mid 2^{341} - 2$; последње својство може бити доказано на следећи начин: имамо $11 \mid 2^{10} - 1 = 1023$, стога $11 \mid 2^{340} - 1$, и $11 \mid 2^{341} - 2$. Следеће, $31 = 2^5 - 1 \mid 2^{340} - 1$, стога је $31 \mid 2^{341} - 2$. Према овоме је број $2^{341} - 2$ дијељив са 11 и 31, а такође и по њиховом производу 341. □

(**Љиљана Госпић 2/17 Д**) задатак преузет са
https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf

28

Доказати за свако n
а) за свако $n \in N$, $\overline{133|11^{n+2} + 12^{2n+1}}^{3^n}$
б) за свако $n \in N$, $\underbrace{aa...a}$ за ма коју цифру a.

Доказ. а) Ово тврђење ћемо доказати математичком индукцијом по n:
Ако је $n = 1$ онда слиједи :
$133|11^{1+2} + 12^{2\cdot 1+1} =$
$1331 + 1728 =$
3059 а то је исто што и
$23 \cdot 133$ а 133 је дјељиво са 133

Претпоставимо да тврђење важи за неко $n \in N$, тада за $n+1$ имамо

$$11^{n+3} + 12^{2n+3} =$$

сада ћемо мало "подесити израз"из првог дијела ћемо извући 11 а из другог 12^2 па ћемо добити овакав израз

$$11 \cdot 11^{n+2} + 144 \cdot 13^{2n+1} = 11 \cdot (11^{n+2} + 12^{2n+1}) + 133 \cdot 12^{2n+1}$$

у претходном кораку смо средили израз тако да смо добили израз из индукцијске претпоставке да тврђење важи за $133|11^{n+3} + 12^{2n+3}$
тако први дио израза је дјељив са 133 због индукцијске претпоставке док други дио јер је 133 дјељиво са 133.
Дакле за свако $n \in N$, $133|11^{n+2} + 12^{2n+1}$.

б) Ово тврђење ћемо такође доказати помоћу математичке индукције по n:
Ако је $n = 1$ онда слиједи :

$$3|\overline{aaa}$$

Претпоставимо да тврђење важи за n па онда имамо да важе : $3^n \,|\overline{\underbrace{aa..a}^{3^n}}$
Сада претпоставимо да тврђење важи за $n+1$.

$$\overline{\underbrace{aa...a}^{3^n+1}} = \overline{\underbrace{aa...a}^{3^n}\underbrace{aa...a}^{3^n}\underbrace{aa...a}^{3^n}} =$$

$$10^{2\cdot 3n}\overline{\underbrace{aa...a}^{3^n}} + 10^{3n}\overline{\underbrace{aa...a}^{3^n}} + \overline{\underbrace{aa...a}^{3^n}} =$$

$$(1\underbrace{00...0}^{3^n-1}1\underbrace{00...0}^{3^n-1}1) \cdot \overline{\underbrace{aa...a}^{3^n}}$$

сада као што смо навели у кораку 2 код индуктивне претпоставке слиједи да је други дио израза тачан , а први дио такође јер :

$$3|1\underbrace{00...0}^{3^n-1}1\underbrace{00...0}^{3^n-1}1$$

тако је овај исказ тачан.

□

(**Милош Ћупић 39/18 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

29

Ако је збир 2004 природна броја дјељив са 6 , онда је и збир њихових кубова дјељив са 6.Доказати.

Доказ. Како је сваки природан број a облика

$$a^3 - a = (a-1)a(a+1)$$

увјек дјељив са 6 , то можемо онда записати и као

$$a_1^3 - a_1 + a_2^3 - a_2 + ... + a_{2004}^3 - a_{2004} =$$

Сада ћемо средити овај израз тако да ћемо раздвојити на једној страни $a_1 + a_2$ і a_{2004} а на другој остатак израза .

$$(a_1^3 + a_2^3 + ... + a_{2004}^3) - (a_1 + a_2 + ... + a_{2004})$$

како је први израз дјељив са 6 онда је и овај израз $(a_1 + a_2 + ... + a_{2004})$ дјељив са 6 а онда је $(a_1^3 + a_2^3 + ... + a_{2004}^3)$ дјељив са 6. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

30

Ако је $(a+b)=1$, онда је $(a+b, a-b)$ једнак 1 или 2.Доказати

Доказ. Рецимо да је :

$$(a+b, a-b) = d$$

Тада можемо да запишемо да је :

$$a+b = d \cdot x$$

$$i$$

$$a-b = d \cdot y$$

Из ове двије једначине добијамо :

$$2 \cdot a = d \cdot (x+y)$$

$$2 \cdot b = d \cdot (x-y)$$

То значи да је d заједнички дјелилац бројева $2a$ и $2b$.
А како су a и b узајамно прости бројеви , то је

$$(2a, 2b) = 2$$

Па је $d|2$, тј $d = 1$ или $d = 2$. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

31

Доказати да је број $= 8888...8(2012 \cdot 2013\text{осмица})$ дјељив бројевима 2,3,7,11,13,37. Провјерити да ли је дјељив и са 4,8,16.

Доказ. За рјешавање овог задатка искористићемо број 888888 , примјећујемо да овај број можемо записати у облику :

$$888888 = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$$

Одакле слиједи да је овај број дјељив са 2,3,7,11,13,37 и са 4 и 8 .
Број А има $2012 * 2013 = 4050156$ цифара а то је уствари $6 * 675026$ цифара. Дакле он се може записати у облику :

$$= 888888 + 10^6 \cdot 888888 + ... + 10^k \cdot 888888 =$$

Сада ћемо издвојити број 888888 испред

$$888888 \cdot (1 + 10^6 + ... + 10^k) =$$

$$8 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot (1 + 10^6 + ... + 10^k)$$

Број 888888 смо записали у облику који смо поменули на почетак рјешавања задатка , одавде је јасно да је број А дјељив са 2,4,8 као и са 3,7,11,13,37 .
Такође видимо да је број у загради непаран па број А није дјељив са 16. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

32

Израчунати А ако је дато да је :

$$2A = 1 + \frac{1}{1+2} + \frac{1}{1+2+3} + ... + \frac{1}{1+2+...+2014}$$

Доказ. За рјешавање овог задатка користићемо формулу за збир првих n бројева :

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$$

и рашчлањивање разломка $\frac{1}{n(n+1)}$ на разлику два разломка на следећи начин :

$$\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$$

За почетак ћемо искористити формулу за збир првих n природних бројева на имениоце који се појављују у задатом изразу. Дакле имамо :

$$1 + 2 = \frac{2 \cdot 3}{2}$$

$$1+2+3=\frac{3\cdot 4}{2}$$

и тако дођемо до :

$$1+2+3+...+2014=\frac{2014\cdot 2015}{2}$$

Када искористимо горе наведене изразе онда нашу једнакост можемо записати на следећи начин :

$$2=1+\frac{1}{\frac{2\cdot 3}{2}}+\frac{1}{\frac{3\cdot 4}{2}}+...+\frac{1}{\frac{2014\cdot 2015}{2}}$$

Сада једноставно се ријешимо двојних разломака тако што измножимо (спољашњи са спољашњим - унутрашњи са унутрашњим)

$$2A=\frac{2}{1\cdot 2}+\frac{2}{2\cdot 3}+\frac{2}{3\cdot 4}+...+\frac{2}{2014\cdot 2015}$$

Добијену једнакост подијелимо са 2 јер имамо 2A добијамо :

$$A=\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+...+\frac{1}{2014\cdot 2015}$$

Сада остаје још да примијенимо растављање разломака који се појављују у овом збиру на разлике по два разломка (на почетку смо поменули формулу коју ћемо користити)

$$=1-\frac{1}{2}+\frac{1}{2}-\frac{1}{3}+\frac{1}{3}-\frac{1}{4}+...+\frac{1}{2014}-\frac{1}{2015}$$

Одузимањем истих разломака добијамо да је :

$$A=1-\frac{1}{2015}$$

Када то мало средимо добијамо :

$$A=\frac{2014}{2015}$$

□

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

33

Ако су у троцифреном броју дељивом са 7 последње две цифре једнаке, доказати да је збир цифара тог броја дељив са 7.

Доказ. Нека су $a, b \in \{0, 1, 2, \ldots, 9\}$, $a \neq 0$ такви да

$$7 \mid \overline{abb} = 100a + 10b + b = 100a + 11b = 98a + 7b + 2(a + b + b).$$

Тада $7 \mid a + b + b$, тј. збир цифара троцифреног броја $\overline{abb}$ дељив је са 7. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

34

Одредити најмањи природан број који при дељењу са 4, 6, 8, 10 и 12 даје остатке редом 2, 4, 6, 8 и 10.

Доказ. Нека је n природан број такав да је $n = 4q_1 + 2$, за неко

$q_1, n = 6q_2 + 4$, за неко q_2, $n = 8q_3 + 6$, за неко q_3, $n = 10q_4 + 8$, за неко q_4, $n = 12q_5 + 10$, за неко q_5.

Тада $4 \mid n + 2, 6 \mid n + 2, 8 \mid n + 2, 10 \mid n + 2, 12 \mid n + 2$, па $[4, 6, 8, 10, 12] \mid n + 2$.

Најмањи природан број такав да $120 \mid n + 2$ ($[\,4,\ 6,\ 8,\ 10,\ 12\,] = 120$) је 118. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

35

Наћи све природне бројеве x,y такве да $y \mid x^2 + 1$ и $x^2 \mid y^3 + 1$.

Доказ. Ако је $x = y$, тада је $x = y = 1$ једно решење. Такође, ако је$y = 2$, тада је $x = 1$ или $x = 3$. Дакле, нашли смо три решења:(1, 1), (1, 2), (3, 2).

Нека је сада (x, y) решење такво да је $x \neq y$ и $y > 2$. Тада су бројеви $\frac{x^2+1}{y}$ и $\frac{y^3+1}{x^2}$ природни и њихов производ је такође природан број. Како је

$$\tfrac{x^2+1}{y} \cdot \tfrac{y^3+1}{x^2} = y^2 + \tfrac{x^2+y^3+1}{x^2y}$$

и број $\frac{x^2+y^3+1}{x^2y}$ је такође природан. Међутим, тада је

$$x^2 + y^3 + 1 \leq x^2 y \Leftrightarrow x^2(y-1) \geq y^3 + 1$$

$$\Leftrightarrow x^2 \geq \tfrac{y^3+1}{y-1} = y^2 + y + 1 + \tfrac{2}{y-1}$$

$$\Rightarrow x^2 \geq y^2 + y + 1 + 1$$

$$\Rightarrow x^2 < (y+1)^2$$

$$\Rightarrow x < y + 1$$

Дакле, ако је (x, y) решење такво да је $x \neq y$ и $y > 2$, тада је $x < y$.
Даље, из $y \mid x^2 + 1$ следи да је $x^2 + 1 = yy_1$, за неки природан број y_1.
Очигледно је $x > 1$. Ако би било $y_1 > x$, имали бисмо

$$yy_1 > (x+1)x = x^2 + x > x^2 + 1,$$

што је немогуће. Дакле, $y1 < x$. Из једнакости $x^2 + 1 = yy_1$ следи да $y1 \mid x^2 + 1$, као и да је $y = \frac{x^2+1}{y_1}$ и

$$y^3 + 1 = \tfrac{(x^2+1)^3}{y_1^3} + 1 = \tfrac{(x^2+1)^3 + y_1^3}{y_1^3},$$

па $x^2 \mid \frac{(x^2+1)^3+y_1^3}{y_1^3}$, одакле следи да $x^2 | (x^2+1)^3 + y_1^3$, тј. да $x^2 \mid y_1^3 + 1$.
На крају имамо да $y_1 \mid x^2 + 1$, $x^2 \mid y_1^3 + 1$ и $y_1 < x$, па мора бити $y_1 \geq 2$. Дакле, проблем се своди на следеће случајеве:

(1) $y_1 = 1$: тада је $y = x^2 + 1$, тј. $x^2 = y - 1$ и $(y-1) \mid y^3 + 1$.
Међутим,

$$y^3 + 1 = y^3 - 1 + 2 = (y-1)(y^2 + y + 1) + 2,$$

па $y - 1 \mid 2$, одакле је $y = 3$, а директном провером видимо да ово није решење.

(2) $y1 = 2$: тада је $2y = x^2 + 1$, тј. $x^2 = 2y - 1$ и $2y - 1 \mid y^3 + 1$, па и $2y - 1 \mid 8y^3 + 8$.
Међутим, из

$$8y^3 + 8 = (2y-1)(4y^2 + 4y + 1) + 9$$

добијамо да $2y - 1 \mid 9$. Тада из $y > 2$, тј. $2y - 1 > 3$, добијамо $y = 5$, одакле директно налазимо да је $x = 3$.
Дакле, решења су: (1, 1), (1, 2), (3, 2), (3, 5).

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

36

Нека је n позитиван цијели број дјељив са 3, 5 и 12. Наћи први број већи од n који је такође дјељив са овим бројевима?

Доказ. Како је број n дјељив са са 3, 5 и 12, то значи да најмањи заједнички садржалац ових бројева дијели број n. Зато ћемо прво наћи најмањи заједнички садржалац бројева 3, 5 и 12.
Прво ћемо дате бројеве да раставимо на просте чиниоце:

$$3 = 3$$

$$5 = 5$$

$$12 = 2 \cdot 2 \cdot 3$$

Или другачије записано:

$$3 = 2^0 \cdot 3^1 \cdot 5^0$$

$$5 = 2^0 \cdot 3^0 \cdot 5^1$$

$$12 = 2^2 \cdot 3^1 \cdot 5^0$$

Сада, да бисмо нашли нзс$(3, 5, 12)$, за сваки од ових простих чиниоца узимамо највећи степен који имамо. Из тога слиједи:

$$\text{нзс}(3, 5, 12) = 2^{max(0,0,2)} \cdot 3^{max(1,0,1)} \cdot 5^{max(0,1,0)}$$

А то је:

$$\text{нзс}(3, 5, 12) = 2^2 \cdot 3^1 \cdot 5^1$$

$$\text{нзс}(3, 5, 12) = 4 \cdot 3 \cdot 5$$

$$\text{нзс}(3, 5, 12) = 60$$

Дакле, број n је дјељив бројем 60, а на основу тога, број n можемо записати у облику:

$$n = 60 \cdot k$$

На основу тога можемо рећи да је сљедећи број који задовољава наше услове и којег ћемо означити са n_2 облика:

$$n_2 = 60 \cdot (k + 1)$$

А то је:

$$n_2 = 60 \cdot k + 60 \cdot 1$$

$$n_2 = 60 \cdot k + 60$$

$$n_2 = n + 60$$

Добили смо да је тражени број n_2 за 60 већи од броја n, односно тај број је: **n+60**. □

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://www.analyzemath.com/numbers/divisibility_questions.html`

37

Доказати да сваки цијели број n важи да је израз

$$(2n+2)^2$$

дјељив бројем 4.

Доказ. Користећи *формулу за квадрат збира* израз $(2+2)^2$ можемо записати у сљедећем облику:

$$(2n+2)^2 = (2n)^2 + 2 \cdot 2n \cdot 2 + 2^2$$

А то је:

$$(2n+2)^2 = 4n^2 + 8n + 4$$

Као што видимо, у изразу $4n^2 + 8n + 4$ имамо заједнички број 4, па њега можемо да издвојимо:

$$(2n+2)^2 = 4(n^2 + 2n + 1)$$

Како је $4(n^2+2n+1)$ дјељиво са 4, из тога слиједи да је и $(2n+2)^2$ дјељиво са 4, чиме смо завршили наш доказ. □

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://www.analyzemath.com/numbers/divisibility_questions.html`

38

Наћи најмањи позитивни двоцифрени цијели број који је дјељив са 3 и збир његових цифара је 9.

Доказ. Како је тражени број двоцифрен, означимо његове цифре са x за цифру десетица и y за цифру јединица. Наш број је тада облика xy. Наш број је дјељив са 3, што значи да се може записати у облику:

$$xy = 3 \cdot k$$

, а из тога можемо да изведемо сљедећу једначину:

$$10x + y = 3k$$

Сљедећи услов каже да је збир цифара једнак 9, односно:

$$x + y = 9$$

Спајањем ове двије једначине добијамо сљедећи систем:

$$\begin{aligned} 10x + y &= 3k \\ x + y &= 9 \end{aligned}$$

У другој једначини нађемо y и замијенимо га у првој:

$$\begin{aligned} 10x + 9 - x &= 3k \\ y &= 9 - x \end{aligned}$$

Сређивањем прве једначине добијамо:

$$9x = 3k - 9$$

Код $3k - 9$ се може издвојити заједничка 3, па читаву једначину можемо подијелити са 3:

$$9x = 3(k - 3) / : 3$$

Затим из једначине нађемо x и означимо је са (1):

$$x = \frac{k-3}{3} (1)$$

Како x означава цифру десетица двоцифреног броја, онда не може бити мање од 1 ни веће од 9. Како тражимо позитиван број различит од 0, онда k мора бити веће од 0. Због тога за k узимамо редом вриједности: 1,2,3,... и мијењамо у једначини *(1)* све док за x не добијемо вриједност из опсега 1-9.
Прва оваква вриједност је $k = 6$. Када њу ставимо у једначину *(1)* добијамо да је $x = 1$. Сад се вратимо у систем једначина и у другој једначини замијенимо x са 1 и добијамо:

$$y = 9 - 1$$

Добијамо да је $y = 8$.
Сада имамо вриједности за x и y и како знамо да је наш тражени број xy облика $10x + y$, добијамо:

$$xy = 10 \cdot 1 + 8$$

Из овога налазимо наш тражени број, а то је **18**.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://www.analyzemath.com/numbers/divisibility_questions.html`

39

Одредити остатак дијељења броја $6^{83} + 8^{83}$ са 49.

Доказ. Запишимо број 6 као 7-1 и број 8 као 7+1 и то запишимо на сљедећи начин:

$$6^{83} + 8^{83} = (7 - 1)^{83} + (7 + 1)^{83}$$

, а то се даље може раставити користећи *биномну формулу*:

$$= 7^{83} - \binom{83}{1} 7^{82} + ... + \binom{83}{82} 7 - 1 +$$

$$7^{83} + \binom{83}{1} 7^{82} + ... + \binom{83}{82} 7 + 1$$

Видимо да су у датом изразу скоро сви бројеви дјељиви са 49.
Нпр. $\binom{83}{1} 7^{82}$ се може записати као $7^2 \cdot \binom{83}{1} 7^{82}$ гдје је $7^2 = 49$.

Једини бројеви који нијесу дјељиви са 49 су: два пута $\binom{83}{82}7$, -1 и 1. 1 и -1 се међусобно поништавају, тако да нам остаје само $2 \cdot \binom{83}{82}7$. Означимо са N број који се добије када се саберу и одузму бројеви добијени дијељењем свих бројева из горњег израза, осим поменутих изузетака, бројем 49. Након тога, додајмо и поменуте изузетке и добићемо горњи израз у облику:

$$N \cdot 49 + 2 \cdot \binom{83}{82} \cdot 7$$

, а то је даље:

$$= N \cdot 49 + 2 \cdot \frac{83!}{82!} \cdot 7$$

$$= N \cdot 49 + 2 \cdot \frac{83 \cdot 82!}{82!} \cdot 7$$

$$= N \cdot 49 + 2 \cdot 83 \cdot 7$$

Број 83 при дијељењу са 7 даје 11 и остатак 6, па га можемо записати:

$$N \cdot 49 + 2 \cdot (11 \cdot 7 + 6) \cdot 7$$

$$= N \cdot 49 + 2 \cdot 11 \cdot 7 \cdot 7 + 2 \cdot 6 \cdot 7$$

$$= N \cdot 49 + 2 \cdot 11 \cdot 49 + 84$$

Сада имамо да само број 84 није дјељив са 49. Покушајмо га раставит овако: $84 = 49 + 35$. Остаје нам 35 који није дјељив са 49, а како њега више не можемо растављати, јер је мањи од 49, то значи да је број 35 наше рјешење, односно остатак при дијељењу $6^{83} + 8^{83}$ са 49 је **35**.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет из књиге Теорија бројева: `https://www.vladimirbozovic.net/univerzitet/bozovic/wp-content/uploads/2010/01/Zbirka-rijesen pdf`

40

Одреди све просте бројеве p за које постоји природни број n такав да су бројеви $n^2 + 3$ и $(n+1)^2 + 3$ дјељиви с p.

Доказ. Претпоставимо да p дијели $n^2 + 3$ и $n^2 + 2n + 4$ за неки $n \in N$. Стога p дијели и њихову разлику:

$$p \mid (n^2 + 2n + 4) - (n^2 + 3) = 2n + 1.$$

Надаље, p дијели и $(2n+1)^2$, а из услова да p дијели $n^2 + 3$ слиједи да p дијели $4(n^2 + 3)$. Одатле слиједи да

$$p \mid (2n+1)^2 - 4(n^2 + 3) = 4n - 11.$$

Сада добијамо

$$p \mid 2(2n+1) - 4(n-11) = 13,$$

pa je $p = 13$ jedini prost broj koji bi mogao zadovoljiti uvjete zadatka. Odredimo još i neki n za koji $13 \mid n^2+3; (n+1)^2+3$. Kako $13 \mid 2n+1$, slijedi da bi "kandidat" za n mogao biti broj 6. Budući da $13 \mid 6^2+3, 7^2+3$ slijedi da je $p = 13$ jedini prost broj za koji vrijede uvjeti zadatka. □

(**Danijela Matanović 38/18 D**) zadatak preuzet sa
https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view

41

Za koje cijele brojeve p jednačina

$$\frac{1}{(x-4)^2} - \frac{p-1}{16-x^2} = \frac{p}{(x+4)^2}$$

ima jedinstveno cjelobrojno rješenje?

Dokaz. Uz uvjet da je $x \neq 4$ i $x \neq -4$, nakon množenja dane jednačine s $(x+4)^2(x-4)^2$ dobijamo:

$$\begin{gathered}(x+4)^2 + (p-1)(x+4)(x-4) = p(x-4)^2,\\ x^2+8x+16+(p-1)(x^2-16) = p(x^2-8x+16),\\ x^2+8x+16+px^2-16p-x^2+16 = px^2-8px+16p,\\ 8x+32-16p = -8px+16p,\\ 8x(p+1) = 32p-32,\ x(p+1) = 4p-4:\end{gathered}$$

Očigledno $p = -1$ nije rješenje. Stoga je $p \neq -1$ i

$$x = \frac{4p-4}{p+1}.$$

Odatle dobijamo

$$x = \frac{4p-4}{p+1} = \frac{4p+4-8}{p+1} = 4 - \frac{8}{p+1}.$$

Da bi rješenje x bilo cjelobrojno, $p+1$ mora dijeliti broj 8. Tada je $p+1 \in \{\pm1, \pm2, \pm4, \pm8\}$, odnosno $p \in \{-9, -5, -3, -2, 0, 1, 3, 7\}$. Zbog početnog uvjeta $x \neq 4$ i $x \neq -4$, p ne smije biti jednak 0. Konačno dobijamo $p \in \{-9, -5, -3, -2, 1, 3, 7\}$ □

(**Danijela Matanović 38/18 D**) zadatak preuzet sa
https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view

42

Ako su a i b rješenja jednačine $x^2 + px - 1 = 0$, gdje je p neparan broj, tada su, za svaki nenegativan cijeli broj n, brojevi $a^n + b^n$ i $a^{n+1} + b^{n+1}$ cijeli i uzajamno prosti. Dokazati.

Доказ. За рјешавање овог проблема потребно је поменути *Виетове формуле*: $a+b=-p$ i $ab=-1$
Доказаћемо тврђење индукцијом.
Узмимо да је $n=0$. Тада имамо:

$$a^n+b^n=a^0+b^0=2$$

$$a^{n+1}+b^{n+1}=a^1+b^1=-p$$

1) Како је број 2 прост и број $-p$ непаран број, самим тим они су узајамно прости бројеви.
2) Сада погледајмо $a^{n+2}+b^{n+2}$ и покушајмо да га представимо преко два његова претходника. То постижемо његовим разлагањем на сљедећи начин:

$$a^{n+2}+b^{n+2}=(a+b)(a^{n+1}+bn+1)-ab(a^n+b^n)$$

Затим, користећи Виетове формуле можемо да замијенимо $(a+b)$ са $-p$ и ab са -1 и добијамо:

$$-p(a^{n+1}+bn+1)+(a^n+b^n)$$

Ово је, такође, цијели број. Ако бројеви $a^{n+2}+b^{n+2}$ и $a^{n+1}+b^{n+1}$ не били узајамно прости, тада не би били узајамно прости ни бројеви $a^{n+1}+b^{n+1}$ и a^n+b^n. То доказује наше тврђење. □

(**Ахмедин Муратовић 22/17 Д**) задатак преузет из књиге Теорија бројева:
`https://www.vladimirbozovic.net/univerzitet/bozovic/wp-content/uploads/2010/01/Zbirka-rijesen`
`pdf`

43

Нека су a, b, c произвољни ненегативни цијели бројеви. Доказати:
а) ако $a \mid b$ и $b \mid c$, тада $a \mid c$
б) ако је $a \mid b$ и $b \neq 0$, тада је $0 <$ a $\leq b$
ц) ако је $a \mid b$ и $a \mid c$, тада, за произвољне цијеле бројеве x и y, $a \mid (bx+cy)$

Доказ. а) Ако $a \mid b$ и $b \mid c$, тада постоје цијели бројеви m и n такви да је $b=ma$ и $c=nb$. Тада је, $c=nma$, а како је mn цио број, слиједи да $a \mid c$. □

Доказ. б) Ako je $a \mid b$, tada postoji nenegativan ceo broj m takav da je $b=ma$. Kako je $b>0$, tada su i a i m pozitivni brojevi, tj. $1 \leq$ a i $1 \leq$ m. Слиједи da je:

$$b=am \geq a \cdot 1=a>0$$

□

Доказ. Ако је $a \mid b$ и $a \mid c$, тада постоје цијели бројеви m и n такви да је $b=m$ и $c=n$. Дакле:

$$bx+cy=max+nay=a(mx+ny)$$

Како је $mx+ny$ цио број, то је $\mid (bx+cy)$. □

(**Јована Шубарић 11/17 Д**) задатак преузет из:
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic
pdf

44

Ако су $a_1, a_2, \ldots, a_n$ позитивни цели бројеви, $n \geq 3$, доказати да је нзд$(a_1, a_2, \ldots, a_n) =$ нзд(нзд$(a_1, a_2, \ldots, a_{n-1})a_n)$

Доказ. Нека је $d =$ нзд$(a_1, a_2, \ldots, a_{n-1})$ и $d' =$ нзд(нзд$(a_1, a_2, \ldots, a_{n-1})a_n)$. Како је $d \mid a_i$, за $i = 1, 2, \ldots, n$, добијамо да је $d \mid$ нзд$(a_1, a_2, \ldots, a_{n-1})$ и $d \mid a_n$. Дакле, $d \mid d'$. Слично, из $d' \mid$ нзд$(a_1, a_2, \ldots, a_{n-1})$ и $d' \mid a_n$ следи $d' \mid a_i$, за $i = 1, 2, \ldots, n$, па добијамо да је $d' \mid d$. Према томе, $d = d'$.
Јасно да је нзд$(a_1, a_2, \ldots, a_n, 0, 0, \ldots, 0) =$ нзд$(a_1, a_2, \ldots, a_n)$.
Закључујемо да се вишеструком применом Еуклидовог алгоритма може добити највећи заједнички делитељ више целих бројева. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic
pdf

45

Ако је n цео број већи од 1, доказати да је n производ простих фактора.

Доказ. Ако је n прост број, тврђење очигледно важи. Претпоставимо да тврђење важи за сваки сложен број мањи од n. Ако је n сложен број, тада постоји цео број d такав да је $1 < d < n$ и $d \mid n$. Означимо са m најмањи такав број. Број m не може бити сложен, јер би у том случају постојао цео број k, такав да је $1 < k < m$ и $k \mid m$, што повлачи да је $k \mid n$. То је, међутим, у контрадикцији са претпоставком да је m најмањи цео број већи од 1 који је делитељ од n. Дакле, m је прост број. Обележимо га са p_1. Следи да је $n = p_1 n_1$, где је $1 < n_1 < n$. По претпоставци индукције број n_1 се може представити у облику простих фактора, према тома, онда може и n. Групишући једнаке преостале факторе броја n, закључујемо да се сваки цео број већи од 1 mможе представити у облику

$$n = \Pi_{i=1}^{k}\, p_i^a i$$

где је $p_1 < p_1 < \cdots < p_k$ и $a_i > 0$, за $i = 1, 2, \cdots, k$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic
pdf

46

Доказати да сваки цео број већи од 1 има јединствен канонски облик.

Доказ. Претпоставимо да постоји позитиван сложен број већи од 1 који се може на два различита начина представити у канонском облику. Нека је n најмањи такав број са представљањима

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

Не постоји прост број p који се појављује у обе канонске репрезентације броја n, јер би у том случају и број $n' = \frac{n}{p}$, који је мањи од n, имао две различите канонске репрезентације, што је у контрадикцији са претпоставком о минималности броја n. Можемо да претпоставимо да је

$$p_1 \leq p_2 \leq \cdots \leq p_k, q_1 \leq q_2 \leq \cdots \leq q_m$$

За просте факторе p_1 и q_1 важи $p_1 \neq q_1$, па можемо узети $p_1 < q_1$.Нека је $N = p_1 p_2 \cdots q_m$.Како је $p_1 \mid N$ и $p_1 \mid n$, следи да је $p_1 \mid (n - N)$, где је $n - N = (q_1 - p_1) \cdot q_2 \cdots q_m > 1$. Следи да се број $n - N$ може написати у облику

$$n - N = p_1 t_1 \cdots t_h,$$

где су t_i прости бројеви за $i = 1, 2, \cdots, h$. Са друге стране, ако је $q_1 - p_1 > 1$, онда се $q_1 - p_1$ може написати као производ простих фактора, на пример $q_1 - p_1 = r_1 \cdot r_2 \cdots r_s$, па добијамо, на други начин, у облику производа простих фактора:

$$n - N = r_1 r_2 \cdots r_s q_2 \cdots q_m$$

Ова последња факторизација не садржи прост фактор p_1. Знамо да је $p_1 \neq q_i$, за $i = 1, 2, \cdots, m$; са друге стране $p_1 \neq r_j$, за $j = 1, 2, \cdots, s$,јер p_1 није делитељ од $q_1 - p_1$. Дакле, број $n - N$ има две различите факторизације, јер само једна од њих садржи прост фактор p_1. То важи и у случају када је $q_1 - p_1 = 1$. Међутим, $1 < n - N < n$ што је у контрадикцији са претпоставком о минималности броја н да не постоји цео број већи од 1, који се може представити на два начина у канонском облику. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic`
`pdf`

47

Ако је цео број b дељив целим бројем $a \neq 0$, доказати да је њихов количник једнозначно одређен.

Доказ. Ако је број b дељив бројем a, онда постоји цео број m као њихов количник, тако да је $b = ma$. Ако би постојао још неки количник n који се добија при дељењу броја b бројем a, онда би важила једнакост $b = na$, па би стога било $ma = na$. Како је $a \neq 0$, из последње једнакости добијамо да је $m = n$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://tesla.pmf.ni.ac.rs/Dmatem/sem3101/Deljivost%20brojeva.pdf`

48

Нека су a, b, c произвољни ненегативни цели бројеви. Доказати да важи:
(a) ако $a \mid b$ и ако је $b \neq 0$, онда је $0 < a \leq b$;
(b) ако $a \mid b$ и $b \mid a$, онда је $a = b$;
(c) ако $a \mid b$ и $b \mid c$, онда $a \mid c$.

Доказ. (a) Ако $a \mid b$, тада по дефиницији постоји ненегативан цео број m такав да је $b = ma$. Како је $b > 0$, бројеви a и m су позитивни, тј. $1 \leq a$ и $1 \leq m$, па је

$$b = ma \geq a\dot{1} = a > 0$$

(b) Претпоставимо да $a \mid b$ и $b \mid a$. Тада је $a \leq b$ и $b \leq c$ на основу тврђења које смо доказали под (a), па је $a = b$ због антисиметричности релације уређења у скупу N.
(c) Ако $a \mid b$ и $b \mid c$, онда постоје цели бројеви m и n такви да је $b = ma$ и $c = nb$. Но онда је $c = nma$, па како је nm цео број, следи да $a \mid b$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://tesla.pmf.ni.ac.rs/Dmatem/sem3101/Deljivost%20brojeva.pdf`

49

Доказати да ако је $a = bq + r$, онда је $(a, b) = (b, p)$

Доказ. Нека је d заједнички дјелилац бројева a и b. Тада из $a = bq + r$ слиједи да $d \mid r$, односно да је d заједнички дјелилац бројева b и r. Ако је c заједнички дјелилац бројева b и r, тада, опет из једнакости $a = bq + r$, слиједи да $c \mid a$, па је c заједнички дјелилац бројева a и b. Према томе, скуп заједничких дјелилаца бројева a и b поклапа се са скупом заједничких дјелилаца бројева b и r, па су међусобно једнаки и њихови највећи елементи, тј. $(a, b) = (b, r)$. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic`
`pdf`

50

Одредити цијеле бројеве α и β такве да је $\alpha \cdot 942 + \beta \cdot 444 = (942, 444)$

Доказ. Прво примјеном Еуклидовог алгоритма добијамо:

$$\begin{aligned} 942 &= 2 \cdot 444 + 54 \\ 444 &= 8 \cdot 54 + 12 \\ 54 &= 4 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned}$$

одакле следи да је $(942, 444) = 6$.
Онда обрнутим Еуклидовим алгоритмом добијамо:

$$\begin{aligned} 54 &= 942 + (-2) \cdot 444 \\ 12 = 444 + (-8) \cdot (942 + (-2) \cdot 444) &= (-8) \cdot 942 + 17 \cdot 444 \\ 6 = 54 + (-4) \cdot 12 &= 33 \cdot 942 + (-70) \cdot 444. \end{aligned}$$

Одатле добијамо: $\alpha = 33, \beta = -70$ □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic`
`pdf`

51

Доказати: $(a, b) \cdot [a, b] = a \mid b$

Доказ. Нека је S заједнички садржалац бројева a и b. Тада је $S = ak$, за неки природан број k. Како $b \mid S$, то је $\frac{ak}{b} \in N$. Нека је $d = (a, b)$.Тада постоје узајамно прости природни бројеви m и n такви да је $a = md$ и $b = nd$, па је:

$$\frac{ak}{b} = \frac{mdk}{nd} = \frac{mk}{n} \in N$$

Како $n \mid mk$ и $(n, m) = 1$, то $n \mid k$, односно постоји природан број t,такав да је $k = nt = \frac{b}{d}t$. Дакле $S = \frac{ab}{d}t$.
С друге стране, сваки број облика $\frac{ab}{d}$ је садржалац бројева a и b. Према томе, S је заједнички садржалац бројева a и b ако и само ако је $S = \frac{ab}{d}t$ $t \in N$.Најмањи такав број добија се за $t = 1$. Дакле, ако је $s = [a, b]$ тада је $s = \frac{ab}{d}$ □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic`
`pdf`

52

Нека су a, b и c цели бројеви такви да важи $a+b+c \mid a^2+b^2+c^2$. Доказати да постоји бесконачно много природних бројева n за које

$$a + b + c \mid a^n + b^n + c^n$$

Доказ. Докажимо индукцијом по броју k да је за све природне бројеве облика $n = 2^k$ испуњено:

$$a + b + c \mid a^n + b^n + c^n,\ a + b + c \mid 2(a^n b^n + b^n c^n + c^n a^n)$$

За $k = 1$ прво тврђење је очигледно, а друго слиједи из

$$2(ab+bc+ca)=(a+b+c)^2-(a^2+b^2+c^2)$$

Нека тврђење важи за неко k. Из

$$a^{2^{k+1}}+b^{2^{k+1}}+c^{2^{k+1}}=(a^{2^k}+b^{2^k}+c^{2^k})^2-2(a^{2^k}b^{2^k}+b^{2^k}c^{2^k}+c^{2^k}a^{2^k})$$

добијамо прво тврђење и за $k+1$, а из

$$a^{2^{k+1}}b^{2^{k+1}}+b^{2^{k+1}}c^{2^{k+1}}+c^{2^{k+1}}a^{2^{k+1}}=(a^{2^k}b^{2^k}+b^{2^k}c^{2^k}+c^{2^k}a^{2^k})^2-2(a^{2^k}+b^{2^k}+c^{2^k})a^{2^k}b^{2^k}c^{2^k}$$

и друго. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic
pdf

53

Ако је $x\cdot p!\cdot q!\cdot r!=2016$ и ако важи да су p,q,r различити природни бројеви већи од 1,одредити бројеве p,q,r,x.

Доказ. Фокусирајмо се за сада на одређивање бројева p,q и r, Како је $2016=2^5\cdot 3^2\cdot 7$, $7!=1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7=5040>2016$ i $5\nmid 2016$, сваки чинилац у p!,q! и r! мора да буде 1,2,3 или 4. Због услова задатка $p<q<r$ лако долазимо до решења.
$4!=1\cdot 2\cdot 3\cdot 4=1\cdot 2\cdot 3\cdot (2\cdot 2)=1\cdot 2\cdot 2\cdot 2\cdot 3=24$
$3!=1\cdot 2\cdot 3=6$
$2!=1\cdot 2=2$
Закључујемо да су решења за p,q,r све пермутације уређене тројке (2,3,4).
Овдје видимо да се број 2 јавља 5 пута у број 3 јавља 2 пута, што одговара поменутом растављању броја 2016. Лако се одређује да је x=7. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://www.pmf.ni.ac.rs/mii-content/2016-3-2/Zadaci%20sa%20brojem%202016.pdf

54

Ако је n прост број,доказати да је број p^4+p^2+1 сложен.

Доказ. Ако је p=2,тада је $p^4+p^2+1=21=3\cdot 7$ што је сложен број. За p=3, $p^4+p^2+1=91=7\cdot 13$, што је такође сложен број.
Докажимо да сваки сложен број има облик $6k\pm 1$, $k\in\mathbb{N}$.
Наиме,ако број p напишемо у облику $p=6k+r$, $0\leq r<6$, тада из услова да је p прост следи да може бити $=1$ или $=5$,одакле произилази тражени закључак. Ако је p прост број облика $6k\pm 1$,тада је број p^4+p^2+1 облика 3m, $m\mathbb{N}$, односно то је сложен број. Дакле за сваки прост број p, број p^4+p^2+1 је сложен. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/12169/mod_resource/content/1/knjiga_DISKRETNA.pdf

55

Наћи најмањи природан број n који има број дјелилаца као број 1998.

Доказ. Како је $1998 = 2 \cdot 3^3 \cdot 37$, укупан број дјелилаца броја 1998 једнак је $\tau(1998) = 2 \cdot 4 \cdot 2 = 16$. Имајући у виду да је $16 = 1 \cdot 16 = 2 \cdot 8 = 4 \cdot 4 = 2 \cdot 2 \cdot 4 = 2 \cdot 2 \cdot 2 \cdot 2$, закључујемо да је број n један од бројева 2^{15}, $2^7 \cdot 3$, $2^3 \cdot 3^3$, $2^3 \cdot 3 \cdot 5$, $2 \cdot 3 \cdot 5 \cdot 7$ (сваки од бројева је, због услова миниммалности броја n, добијен множењем најмањих могућих простих бројева).
Од наведених бројева, најмањи је број $2^3 \cdot 3 \cdot 5 = 120$ и то је тражени број. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/12169/mod_resource/content/1/knjiga_DISKRETNA.pdf

56

Доказати да $2^{50} + 1$ није дјељиво са $2^7 - 1$

Доказ. Примјетимо да је $2^7 \equiv 1 \pmod{2^7 - 1}$, па је $2^{50} \equiv 2 \pmod{2^7 - 1}$ □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imomath.com/srb/dodatne/uvodkongr_mr.pdf

57

Доказати да се разломак $\frac{12n+1}{30n+2}$ не може даље скратити.

Доказ. Да бисмо показали да се разломак не може скратити,показаћемо да је нзд$(12n + 1, 30n + 2) = 1$
Kako je:
$5(12n + 1) - 2(30n + 2) = 60n + 5 - 60n - 4 = 1$
$\Rightarrow$ нзд$(12n + 1, 30n + 2) = 1$ □

(**Николина Јеловац 13/18 Д**) задатак преузет са
предавања професора Владимира Божовића
(**Лука Брацовић 17/17 Д**) задатак преузет са:
http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=6024B41025E64542A29E9485D93358EA?doi=10.1.1.649.6499&rep=rep1&type=pdf

58

Доказати да је $n^3 - n$ увијек дјељиво са 3.

Доказ. Испитаћемо овај проблем из 3 дијела тако што ћемо n записати као: $n = 3k$, $n = 3k + 1$ і $n = 3k + 2$ и појединачно тумачити да ли су дјељиви са 3. Уколико су сва три записа дјељива са 3, онда је и само $n^3 - n$ дјељиво са 3.

а) Уврстимо $n = 3k$ у $n^3 - n$:

$$(3k)^3 - 3k = 27k^3 - 3k = 3(9k^3 - k)$$

Закључујемо да је $n^3 - n$ је дјељиво са 3 за $n = 3k$.

б) Уврстимо $n = 3k + 1$ у $n^3 - n$:

$$(3k + 1)^3 - (3k + 1) = 27k^3 + 27k^2 + 9k + 1 - 3k - 1 = 3(9k^3 + 9k^2 + 2k)$$

Закључујемо да је $n^3 - n$ је дјељиво са 3 за $n = 3k + 1$.

в) Уврстимо $n = 3k + 2$ у $n^3 - n$:

$$(3k + 2)^3 - (3k + 2) = 27k^3 + 54k^2 + 36k + 8 - 3k - 2 = 3(9k^3 + 18k^2 + 11k + 2)$$

Закључујемо да је $n^3 - n$ је дјељиво са 3 за $n = 3k + 2$.

Самим тим што су сва три записа дјељива са 3, закључујемо да је $n^3 - n$ увијек дјељиво са 3. Тиме је овај доказ завршен. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

59

Са колико нула се завршава број који се добија множењем првих 2016 природних бројева?

Доказ. $1 \cdot 2 \cdot 3 \cdots 2015 \cdot 2016 = 2016!$
Цифра 0 се у производу добија множењем бројева 2 и 5, као и њихових степена. С обзиром да је број степена броја 5 мањих од 2016 мањи него број степена броја 2 мањих од 2016, бројаћемо дјелиоце бројева $5, 5^2, 5^3$ и 5^4 јер су то једини степени броја 5 мањи од броја 2016.

Број нула којима се број 2016 завршава добија се као збир појединачних количника броја 2016 и степена броја 5 мањих од броја 2016 заокружених на најближим цијелим бројевима мањим од добијених количника.

Дакле:

$$\lfloor(2016/5)\rfloor + \lfloor(2016/25)\rfloor + \lfloor(2016/125)\rfloor + \lfloor(2016/625)\rfloor = 403 + 80 + 16 + 3 = 502$$

Рјешење: Број који се добија множењем првих 2016 природних бројева се завршава са 502 нуле. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=6024B41025E64542A29E9485D93358EA?doi=10.1.1.649.6499&rep=rep1&type=pdf`

60

Доказати да се сваки квадрат броја може записати у облицима $4k$ или $4k+1$.

Доказ. Сваки цијели број се може записати као $2x$ или $2x+1$.

Уколико је $n = 2x$ онда је $n^2 = 4x^2$. Узмимо да је $k = x^2$ и добијамо да је $n^2 = 4k$.

Слична процедура је и код другог случаја.

За $n = 2x+1$ важи да је $n^2 = 4x^2 + 4x + 1 = 4(x^2 + x) + 1$. Узмимо да је $k = x^2 + x$ и добијамо да је $n^2 = 4k + 1$.

Овим је доказано да се сваки квадрат броја може записати у облицима $4k$ или $4k+1$. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=6024B41025E64542A29E9485D93358EA?doi=10.1.1.649.6499&rep=rep1&type=pdf`

61

Доказати да је $\sqrt{2}$ ирационалан број.

Доказ. Претпоставимо да се $\sqrt{2}$ може записати као $\sqrt{2} = p/q$, за $p, q \in N$.

Такође, претпоставимо да су p и q узајамно прости. Помножимо $\sqrt{2} = p/q$ са q и квадрирајмо обије стране и добијамо $2q^2 = p^2$.

Одавде закључујемо да $2 \mid p^2$. Самим тим важи и $2 \mid p$ јер квадрат неког броја је паран само ако је и тај број паран$((2k)^2 = 2(2k^2))$.

P записујемо као $2k$ за $k \in N$. Уврстимо то и добијамо да $2q^2 = (2k)^2$ што се може скратити на $q^2 = 2k^2$.

Из овога се да закључити да $2 \mid q^2$ а затим и да $2 \mid q$ на истом основу као и са p.

Закључујемо да је број 2 заједнички дјелилац бројева p и q чиме долази до контрадикције са претпоставком да су узајамно прости. Овим је доказано да се $\sqrt{2}$ не може записати као разломак два цијела броја тј. доказано је да је $\sqrt{2}$ ирационалан број. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

62

Доказати да је за сваки природан број n бар један од бројева $3^{3n} + 2^{3n}$ и $3^{3n} - 2^{3n}$ дјељив са 35.

Доказ. Треба провјерити два случаја, када је n паран и када је непаран.

а) Непаран:

$$n = 2k + 1 \implies 3^{6k+3} + 2^{6k+3} = (3^9 + 2^9)M = 20195M$$

С обзиром да је 20195 дјељиво са 35, закључујемо да је за сваки непаран број број $3^{3n} + 2^{3n}$ дјељив са 35.

б) Паран:

$$n = 2k \implies 3^{6k} - 2^{6k} = (3^6 - 2^6) = 665M$$

Како је 665 такође дјељиво са 35, слиједи да је за сваки паран број број $3^{3n} - 2^{3n}$ је дјељив са 35.

Тиме је доказ завршен. □

63

Нека је n природан број. Доказати да је број $(n+1)(n+2)\dots(n+n)$ дјељив са 2^n, а није дјељив са 2^{n+1}.

Доказ. Доказаћемо индукцијом да се број 2 појављује тачно n пута као чинилац броја $(n+1)(n+2)\dots(n+n)$.
За $n=1$ тврђење је очигледно тачно, јер је тада дати производ једнак 2. Претпоставимо да се, за неки природан број n, број 2 у производу $(n+1)(n+2)\dots(n+n)$ појављује као чинилац тачно n пута.
Тада је

$$\begin{aligned}&(n+1+1)(n+1+2)\dots(n+1+n-1)(n+1+n)(n+1+n+1)\\&=(n+2)(n+3)\dots(n+n)(2n+1)(2n+2)\\&=(n+2)(n+3)\dots(n+n)(2n+1)2(n+1)\\&=2(n+1)(n+2)(n+3)\dots(n+n)(2n+1)\end{aligned}$$

па пошто се, према индукцијској претпоставци, 2 појављује тачно n пута као чинилац у производу $(n+1)(n+2)\dots(n+n)$, а чинилац $2n+1$ је непаран па он није дјељив са 2, слиједи да се у производу $(n+1+1)(n+1+1)\dots(n+1+n-1)(n+1+n)(n+1+n-1)$ број 2 као чинилац појављује тачно $n+1$ пута. □

(**Никола Цупара 08/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

64

Одредити све парове (a,b) природних бројева, такве да је број a^2b+a+b дјељив са ab^2+b+7.

Доказ. Нека пар (a,b) задовољава услов задатка, тј. нека

$$ab^2+b+7|a^2b+a+b.$$

Размотримо најпре случајеве $b=1$ и $b=2$.
За $b=1$ добијамо да се $a+8|a^2+a+1$.
Како је $a^2+a+1=(a+8)(a-7)+57$, то $a+8|57=3\cdot 19$, постоје две могућности $a=11$ и $a=49$. Провјером се показује да парови (11,1) и (49,1) задовољавају услов задатка.
За $b=2$ добијамо услов $4a+9|2a^2+a+2$.
Како је $8(2a^2+a+2)=(4a+9)(4a-7)+79$ слиједи да $4a+9|79$, што је очигледно немогуће, па у овом случају нема решења.
Нека је сада $b\geq 3$. Како је

$$b(a^2b+a+b)=a(ab^2+b+7)+b^2-7a,$$

□

(**Никола Цупара 08/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

65

Наћи највећи петоцифрени палиндром који је дјељив са 101.

Доказ. Било који петоцифрени палиндром $\overline{abcba}$ може се приказати у облику

$$\overline{abcba} = 10001a + 1010b + 100c = 101(99a + 10b + c) + 2a - c.$$

То значи да је тај палиндром дјељив са 101 акко је $2a - c = 0$ (јер је за било које цифре a и c испуњено $|2a - c| < 101$). Једначина $2a = c$ имплицира да је $a \leq 4$. Пошто тражимо највећи број, узећемо да је $a = 4$. Тада је $c = 8$. Како за цифру b немамо никакве услове, можемо узети $b = 9$ да бисмо добили највећи могући број. Дакле, тражени број је 49 894. □

(**Никола Цупара 08/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

66

Факторизација сваког природног броја $n > 1$ на просте факторе је јединствена до на поредак простих фактора.

Доказ. Претпоставимо да n има двије различите факторизације.Дијелећи са простим бројевима који су заједнички обијема репрезентацијама, добићемо једнакост облика

$$p_1 p_2 \dots pr = q_1 q_2 \dots q_s,$$

гдје су p_i, q_j прости бројеви, не нужно различити, али такви да се нити један прост број са лијеве стране не појављује на десној страни, тј. $p_i \neq q_j$ за све i, j. Међутим, то је немогуће јер из $p_1 \mid q_1 q_2 \dots q_s$, слиједи па p_1 дијели барем један q_j. Но, то значи да је $p_1 = q_j$, контрадикција.

□

(**Никола Цупара 08/17 Д**) задатак преузет са:
`https://www.academia.edu/2991414/Uvod_u_teoriju_brojeva_skripta_`

67

Доказати да $21|a^2 + b^2$ повлачи $441|a^2 + b^2$.

Доказ. Како $21|a^2+b^2$, то $3|a^2+b^2$ и $7|a^2+b^2$. Како су остаци квадрати при дељењу са 3 или 0 или 1, то и a и b морају бити дељиви са 3, па је a^2+b^2 дељиво са 9. Такође, како квадрати при дељењу са 7 дају остатке 0,1,2 и 4, то и a и b морају бити дељиви са 7, па је a^2+b^2 дељиво са 49. Значи $9 \cdot 49 = 441|a^2+b^2$.

□

(**Никола Цупара 08/17 Д**) задатак преузет са:
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

68

Од 156 играчака, 234 јабуке и 390 чоколадица направљен је највећи могући број новогодишњих пакетића. Колико кошта један пакетић ако је цена играчке 250 динара, јабуке 15 динара, а чоколадице 12 динара?

Доказ.

$$\begin{aligned} 156, 234, 390 &| 2 \\ 78, 117, 195 &| 3 \\ 26, 39, 65 &| 13 \\ 2, 3, 5 &| \\ 2 \cdot 3 \cdot 13 = 78^{\smile} & \end{aligned}$$

$$\begin{aligned} 2 &- \\ 3 &- j \\ 5 &- \end{aligned}$$

□

(**Јакша Мрдак 23/17 Д**)

69

Колики је количник q и остатак при дјељењу броја 215 са бројем 11?

Доказ. Поделимо дате бројеве: $215/11 = 19(6)$
$q = 19$ а остатак $r = 6$.
Важи једнакост:
$215 = 19 * 11 + 6$

□

(**Јакша Мрдак 23/17 Д**)

70

Одреди вредност цифре x тако да број $27 * 5$ буде дељив са бројем 3.

Доказ. Број је дељив са 3, ако му је збир цифара дељис са три. Без цифре x, збир је $2+7+5=14$. До првог дељивог са 3 недостаје 1, па цифра x може бити баш 1. Може бити и 4 или 7 јер је у сваком случају добијени збир дељив са 3. Дакле,

X елемент $1, 4, 7$

□

(**Јакша Мрдак 23/17 Д**)

71

Број 82 напиши у облику збира два броја тако да када се већи број подели мањим буде количник 3 и остатак 2.

Доказ. $82 : A + B = 82$

Примјеном једнакости дјељивости:
$a = b * q + r$ биће:
$A : B = 3(2)$
$A = 3(B) + 2$
Збир бројева је сад
$3B + 2 + B = 82$
$4B + 2 = 82$
$4B = 82 - 2$
$4B = 80$
$B = 20$
$A = 82 - 20 = 62$

□

(**Јакша Мрдак 23/17 Д**)

72

Наћи бар једно цјелобројно решење једначине $936x + 588y = 12$.

Доказ. Како је $(936, 588) = 12$, за решавање задате једначине примијенићемо процедуру:

$$12 = 108 - 4 \cdot 24 =$$

$$= 108 - 4 \cdot (240 - 2 \cdot 108) =$$

$$= 9 \cdot 108 - 4 \cdot 240 =$$

$$= 9 \cdot (348 - 240) - 4 \cdot 240 =$$

$$= 9 \cdot 348 - 13 \cdot 240 =$$

$$= 9 \cdot 348 - 13 \cdot (588 - 348) =$$

$$= 22 \cdot 348 - 13 \cdot 588 =$$

$$= 22 \cdot (936 - 588) - 13 \cdot 588 =$$

$$= 22 \cdot 936 - 35 \cdot 588.$$

Једно цјелобројно решење једначине је $x = 22, y = -35$. Нека је сада f произвољан дјелилац бројева и b. Тада су $\frac{a}{f}$ и $\frac{b}{f}$ цијели бројеви, па важи:

$$\frac{a}{f}x + \frac{b}{f}y = \frac{(a,b)}{f}$$

одакле слиједи да је израз на десној страни посљедње једнакости цио број. То онда значи да $f|(a,b)$. □

(**Андреа Ђурашковић 14/17, Д**) задатак преузет са:
`http://operator.pmf.ni.ac.rs/www/pmf/publikacije/Mii/2008-2009/broj%201%20sveska%201-2/mii1-4.pdff`

73

Доказати да $n^2 + 23$ је дјеливо са 24 за бесконачаноп много n-ова

Доказ. Примјећујемо да можемо да напишемо $n^2 + 23$ као $(n-1)(n+1) + 24$

Из тога можемо да изразимо n као $n = 24k \pm 1$, $k = 0, 1, 2...$

Из тога слиједи да за било које k, наш израз ће бити дјељив са 24

□

(**Филип Станковић 5-17 Д**) задатак преузет са:
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

74

Наћи све природне бројеве за које важи $n+1|n^2+1$

Доказ. Наш израз $n^2+1 = n(n+1)$ можемо да сведемо на $n^2+1 = n(n+1)-(n-1)$

Дакле, ако $n+1|n^2+1$, онда $n+1|n-1$, што за природан број n је могуће само ако $n-1=0$

што значи да је наше решење $n=1$ □

(**Филип Станковић 5-17 Д**) задатак преузет са:
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

75

Доказати да за сваки природан број n број $3(1^5+2^5+...+n^5)$ је дјељив са $1^3+2^3+...+n^3$

Доказ. Коришћењем математичке индукције, можемо да изведемо:

$1^3+2^3+...+n^3 = \frac{n^2(n+1)^2}{4}$

Поновним коришћењем математичке индукције, добијамо да је

$1^5+2^5+...+n^5 = \frac{1}{12}n^2(n+1)^2(2n^2+2n-1)$

Из изведених формула, примјећујемо да обије формуле имају чиниоц $\frac{n^2(n+1)^2}{4}$ у себи, што доказује да су међусобно дјељиви

□

(**Филип Станковић 5-17 Д**) задатак преузет са:
`https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

76

Доказати да $16|(a^4+b^4-2)$ за све непарне природне бројеве a и b.

Доказ. Почињемо тако што пишемо a^4+b^4-2 као $(a^4-1)+(b^4-1)$.Видимо да (a^4-1) можемо да запишемо као $(a^2-1)(^2+1)$. Из тога слиједи $(a-1)(+1)(^2+1)$. Обзиром да знамо да је a непарно, можемо да пишемо $a=2k+1$ и из тога добијамо:

$$(a-1)(a+1)(a^2+1) = (2k)(2k+2)(4k^2+4k+1) = 8k(k+1)(2k^2+2k+1)$$

Доказали смо да је наш израз дјељив са 8, међутим наш цил је да докажемо да је израз дјељив са 16. Ако обратимо пажњу, у изразу имамо $k(k+1)$, из чега можемо да закључимо да је k или $k+1$ паран број, а паран број помножен са 8 мора бити дјељив са 8

Значи, доказали смо да $^4 - 1$ је дјељиво са 16, самим тим смо доказали и да је $^4 - 1$ дјељиво са 16,
и из тога слиједи да је $a^4 + b^4 - 2$ дјељиво са 16, јер је збир 2 броја дјељива са 16 дјељив са 16

□

(**Филип Станковић 5/17 Д**) задатак преузет са
`http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=6024B41025E64542A29E9485D93358EA?doi=10.1.1.649.6499&rep=rep1&type=pdf`

2 Конгруенције - рачун остатака

77

Наћи остатак при дијељењу 2^{678} са 11.

Доказ. Да бисмо добили решење задатка, неопходно је да израчунамо чему је 2^{678} конгруентно по модулу 11. Дакле, слиједи:

$$2^1 \equiv 2 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 2^3 \equiv 8 \pmod{11}, \quad 2^4 \equiv 5 \pmod{11},$$
$$2^5 \equiv 10 \pmod{11}, \quad 2^6 \equiv 9 \pmod{11}, \quad 2^7 \equiv 7 \pmod{11}, \quad 2^8 \equiv 3 \pmod{11},$$
$$2^9 \equiv 6 \pmod{11}, \quad 2^{10} \equiv 1 \pmod{11}$$

Сада је

$$2^{670} = (2^{10})^{67} \equiv 1^{67} \equiv 1 \pmod{11},$$

па је

$$2^{678} = 2^{670} \cdot 2^8 \equiv 1 \cdot 3 \equiv 3 \pmod{11}$$

Добили смо да је остатак при дијељењу 2^{678} са 11 једнак 3.

□

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://elib.mi.sanu.ac.rs/files/journals/mk/7/mkn7p27-36.pdf`

78

Бројеви a и b имају исте остатке при дијељењу са m, акко је $a \equiv b \pmod{m}$.

Доказ. Ако је $a \equiv b \pmod{m}$, тада постоји цио број t, такав да је $a = b + mt$. За b и $m \neq 0$ постоје једнозначно одређени цијели бројеви q и r, такви да је $b = mq + r$, $0 \leq r <\mid m \mid$, гдје је r остатак добијен при дијељењу b са m. Одавде слиједи да је $a = m(t+q)+r, 0 \leq r <\mid m \mid$. Дакле и број a има исти остатак при дијељењу са m.

Обратно, нека су a и b бројеви који при дијељењу са m имају исте остатке. Тада се може записати да је $a = mg_1 + r$ и $b = mg_2 + r$, при чему је $0 \leq r <| m |$. Одавде слиједи да је $a - b = m(q_1 - q_2)$, па је $a \equiv b \pmod{m}$. □

(**Катарина Синђић 36/19 Д**) задатак преузет са `https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic.pdf`

79

(а) Нека су a, b, c цијели бројеви и n је природан број. Нека су бројеви a и n релативно прости. Ако је $ab \equiv ac \pmod{n}$, тада је $b \equiv c \pmod{n}$.
(б) Нека је $ax \equiv ay \pmod{n}$. Тада је $x \equiv y \pmod{\frac{n}{d}}$, гдје је $d = (a, n)$.

Доказ. (а) Како су a и n релативно прости, постоје цијели бројеви x и y, такви да је (*) $ax + ny = 1$. Из конгруенције $ab \equiv ac \pmod{n}$, слиједи да постоји цијели број k, такав да је $a(b-c) = nk$. Из (*) је $ax = 1 - ny$. Када претходну једнакост помножимо са x, добијамо да је $ax(b-c) = nkx$. У ax замијенимо $1 - ny$ и онда је $(1 - ny)(b-c) = nkx$, односно добијамо $(b-c) - ny(b-c) = nkx$. Очигледно је да n дијели $b - c$, па је $b \equiv c \pmod{n}$, чиме је доказ завршен.

(б) Како је $ax \equiv ay \pmod{n}$, постоји цијели број k, такав да је $ax - ay = kn$. Одатле је $\frac{a}{d}(x - y) = \frac{nk}{d}$, па $\frac{n}{d} \mid \frac{a}{d}(x - y)$. Него, како су $\frac{n}{d}$ и $\frac{a}{d}$ релативно прости, јер немају заједничких простих фактора, добијамо $\frac{n}{d} \mid (x - y)$, чиме је тврђење доказано. □

(**Катарина Синђић 36/19 Д**) задатак преузет са `http://www.mathos.unios.hr/~imatic/uvod%20u%20teoriju%20brojeva%20prvi%20dio.pdf`

80

Доказати да је број $3^{105} + 4^{105}$ дјељив са 13, а није дјељив са 11.

Доказ. Имамо $3^{105} = (3^3)^{35} = 27^{35}$ и $4^{105} = (4^3)^{35} = 64^{35}$, па можемо написати:

$$\begin{aligned} 3^{105} + 4^{105} &\equiv 27^{35} + 64^{35} \pmod{13} \\ &\equiv (26 + 1)^{35} + (65 - 1)^{35} \\ &\equiv 1^{35} + (-1)^{35} \\ &\equiv 0 \pmod{13} \end{aligned}$$

Одавде добијамо да је број дјељив са 13. Међутим,

$$\begin{aligned} 3^{105} + 4^{105} &= 3 \cdot (11 - 2)^{52} + (66 - 2)^{35} \\ &\equiv 3 \cdot 2^{52} - 2^{35} \pmod{11} \\ &\equiv 12 \cdot 32^{10} - 32^7 \\ &\equiv 12 \cdot (-1)^{10} - (-1)^7 \\ &\equiv 12 + 1 \equiv 2 \pmod{11} \end{aligned}$$

Дакле, добијамо да број $3^{105}+4^{105}$ није дјељив са 11. □

(**Катарина Синђић 36/19 Д**) задатак преузет са `https://www.fer.unizg.hr/_download/repository/diskont1-11.pdf`

81

(а) Одредити последњу цифру броја 7^{7^7}.
(б) Одредити двије последње цифре броја 9^{9^9}.
(в) Наћи остатак при дијељењу квадрата непарног цијелог броја са 8.

Доказ. (а) Како је $7 \equiv -1 \pmod 4$, то је $7^{7^7} \equiv -1 \pmod 4$, јер је 7^7 непаран број. Дакле, $7^{7^7} = 4k+3$, за неки природан број k.

Пошто је $7^2 \equiv -1 \pmod{10}$, то је $7^4 \equiv 1 \pmod{10}$, па је и $7^{4k} \equiv 1 \pmod{10}$. Дакле,

$$7^{7^{7^7}} = 7^{4k+3} = 7^{4k} \cdot 7^3 \equiv 7^3 \equiv 3 \pmod{10}.$$

Последња цифра броја $7^{7^{7^7}}$ је 3.

(б) Како је

$$9^{10} = (10-1)^{10} \equiv 1 \pmod{100} \implies 9^{10q+r} \equiv 9^r \pmod{100}.$$

Даље, како је

$$9^9 \equiv 9 \pmod{10} \implies 9^{9^9} \equiv 9^9 \equiv 89 \pmod{100}.$$

Према томе, последње двије цифре броја 9^{9^9} су 8 и 9.

(в) Непаран број можемо записати као $2n+1$. За сваки природан број n је

$$(2n+1)^2 = 4n^2+4n+1 = 4n(n+1)+1,$$

па, како $8 \mid 4n(n+1)$ јер ($2 \mid n(n+1)$), то је остатак при дијељењу $(2n+1)^2$ са 8 једнак 1, тј. $(2n+1)^2 \equiv 1 \pmod 8$. Дакле, остатак при дијељењу квадрата непарног цијелог броја са 8 је 1.

□

(**Катарина Синђић 36/19 Д**) задатак преузет са `https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf`

82

(а) Одредити последње три цифре збира бројева $1^{2012}+2^{2012}+\ldots 1000^{2012}$.
(б) Одредити остатак при дијељењу броја 2^{p^2} са 13, ако се зна да је p прост број већи од 3.

Доказ. (а) Последње три цифре представљају остатак при дијељењу броја са 1000. Очигледно је

$$1000^{2011} \equiv 0 \pmod{1000}$$

и

$$500^{2011} \equiv 0 \pmod{1000}.$$

На основу тога, даље је:

$$999^{2011} \equiv (-1)^{2011} = -1^{2011} \pmod{1000}.$$

По истом принципу можемо закључити:

$$998^{2011} \equiv (-2)^{2011} = -2^{2011} \pmod{1000}$$

Све ово можемо уопштити на следећи начин:

$$(100-k)^{2011} \equiv (-k)^{2011} = -k^{2011} \pmod{1000} (k \in \mathbb{N}, k < 1000).$$

Сабирајући бројеве, долазимо до следећег закључка:

$$1^{2011} + 2^{2011} + \cdots + 499^{2011} + 500^{2011} + 501^{2011} + \cdots + 998^{2011} + 999^{2011} + 1000^{2011}$$
$$\equiv 1^{2011} + 2^{2011} + \cdots + 499^{2011} + 0 - 499^{2011} - \ldots 2^{2011} - 1^{2011} + 0 = 0 \pmod{1000}.$$

Закључујемо да је троцифрени завршетак 000.

(б) Ако је p прост број и $p > 3$, онда је p облика $6k-1$ или $6k+1 (k \in \mathbb{N})$. Како је

$$(6k \pm 1)^2 = 36k^2 \pm 12k + 1,$$

то значи да p^2 при дијељењу са 12 даје остатак 1. Како је

$2^{12} = (2^6)^2 = (64)^2 \equiv (-1)^2 = 1 \pmod{13}$, па је

$2^{p2} = 12^{12m+1} = (2^{12})^m \cdot 2 \equiv 1^m \cdot 2 = 2 \pmod{13}$. Дакле, остатак је 2.

(**Катарина Синђић 36/19 Д**) задатак преузет са `https://informatematika.weebly.com/uploads/2/6/6/2/26628539/kongruencije-po-modulu.pdf`

□

83

Ријешимо конгруенцију $555 \cdot x \equiv 15 \pmod{500}$.

Доказ. Будући да је $(555, 5005) = 5$ и $5 \mid 15$, треба ријешити конгруенцију

$$111 \cdot x \equiv 3 \pmod{1001}.$$

Примијенимо Еуклидов алгоритам:

$$\begin{aligned} 1001 &= 111 \cdot 9 + 2 \\ 111 &= 2 \cdot 55 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

Дакле, рјешење конгруенције $111u \equiv 1 \pmod{1001}$ је $u \equiv 496 \pmod{1001}$. Стога је рјешење од $111x \equiv 3 \pmod{1001}$, $x \equiv 1488 \equiv 487 \pmod{1001}$. Коначно, рјешење полазне конгруенције је

$$x \equiv 487, 1488, 2489, 3490, 4491 \pmod{5005}.$$

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`https://www.academia.edu/2991414/Uvod_u_teoriju_brojeva_skripta_`

84

Нека су a, b, c, d цијели бројеви.
(1) Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, онда је $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}, ac \equiv bd \pmod{m}$.
(2) Ако је $a \equiv b \pmod{m}$ и $d|m$, онда је $a \equiv b \pmod{d}$.
(3) Ако је $a \equiv b \pmod{m}$, онда је $ac \equiv bc \pmod{mc}$ за сваки $c \neq 0$.

Доказ. (1) Нека је $a - b = mk$ и $c - d = ml$. Тада је $(a + c) - (b + d) = m(k + l)$ и $(a - c) - (b - d) = m(k - l)$, па је $a + c \equiv b + d \pmod{m}$ и $a - c \equiv b - d \pmod{m}$. Због $ac - bd = a(c - d) + d(a - b) = m(al + dk)$ слиједи да је $ac \equiv bd \pmod{m}$.

(2) Нека је $m = dc$. Тада из $a - b = mk$ слиједи $a - b = d \cdot (ek)$, па је $a \equiv b \pmod{d}$.

(3) Из $a - b = mk$ слиједи $ac - bc = (mc) \cdot k$, па је $ac \equiv bc \pmod{mc}$.

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`https://www.academia.edu/2991414/Uvod_u_teoriju_brojeva_skripta_f`

85

Одредити остатак при дијељењу броја $(7^{2012})^{2014} - (3^{12})^{14}$ са 10.

Доказ. Будући да је нзд$(7, 10) = 1$, према Ојлеровој теореми слиједи:

$$7^{\phi(10)} = 7^4 \equiv 1 \pmod{10}$$

па је

$$7^{2012} \equiv 1 \pmod{10}$$

$$(7^{2012})^{2014} \equiv 1 \pmod{10}$$

Аналогно,

$$3^{\phi(10)} = 3^4 \equiv 1 \pmod{10},$$

из чега слиједи да је

$$(3^{12})^{14} \equiv 1 \pmod{10}.$$

Имамо да је $(7^{2012})^{2014}$ - $(3^{12})^{14} \equiv 0 \pmod{10}$ па закључујемо да је остатак броја $(7^{2012})^{2014}$ - $(3^{12})^{14}$ при дијељењу са 10 једнак 0. □

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

86

Доказати да је број $2222^{5555} + 5555^{2222}$ дјељив са 7.

Доказ. Како је $2222 \equiv 3 \pmod{7}$, $3^6 \equiv 1 \pmod{7}$ и $5555 \equiv 5 \pmod{6}$, то је

$$2222^{5555} = 2222^{6\cdot 925+5} = (2222^6)^{925} \cdot 2222^5 \equiv (3^6)^{925} \cdot 3^5 \equiv 1 \cdot 3^5 \pmod{7}.$$

Слично из,

$$5555 = 4 \pmod{7},\ 4^3 \equiv 1 \pmod{7} \text{ и } 2222 \equiv 2 \pmod{3}$$

следи:

$$5555^{2222} = 5555^{3\cdot 740+2} \equiv 4^2 \equiv 2 \pmod{7}.$$

Сада се тврђење добија из

$$2222^{5555} + 5555^{2222} \equiv 5 + 2 \pmod{7}.$$

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

87

Доказати да је цифра стотина броја $2^{1999} + 2^{2000} + 2^{2001}$ парна.

Доказ. Запишимо број у облику

$$2^{1999} \cdot (1 + 2 + 4) = 7 \cdot 2^9 \cdot 2^{10} \cdot 2^{1980} = 7 \cdot 2^9 \cdot 2^{10} \cdot (2^{20})^{99}.$$

Пошто је $2^9 = 512$, $2^{10} = 1024$ и $2^{20} = (2^{10})^2$ то се двоцифрени завршетак броја 2^{20} поклапа са двоцифреним завршетком броја 24^2, па је двоцифрени завршетак броја 2^{20} једнак 76. Двоцифрени завршетак броја 76^2 је такође 76, па је двоцифрени завршетак датог броја једнак двоцифреном завршетку производа $7 \cdot 12 \cdot 24 \cdot 76$, а то је 16. Пошто је број $2^{1999} + 2^{2000} + 2^{2001}$ дјељив са 8, а двоцифрени завршетак му је 16, па цифра стотина мора бити парна.

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

88

Ако су природни бројеви x и y такви да су бројеви $3x+4y$ и $4x+3y$ потпуни квадрати, доказати да су и x и y дјељиви са 7.

Доказ. Нека је:

$$(1) \qquad 3x + 4y = m^2, \;\; 4x + 3y = n^2.$$

Тада

$$(2) \qquad 7(x + y) - m^2 + n^2 \Rightarrow 7 \mid m^2 + n^2.$$

Узимајући $m = 7k + r, r \in \{0, 1, 2, 3, 4, 5, 6\}$ добијамо да су $0, 1, 2, 3, 4$ могући остаци при дељењу квадрата целог броја са 7. Сада лако закључујемо да је $m^2 + n^2 \equiv 0 \pmod 7$ ако и само ако су и m и n дељиви са 7, па је тада

$$m^2 + n^2 \equiv 0 \pmod{7^2},$$

тј. $7(x + y) \equiv 0 \pmod{7^2}$, одакле добијамо

$$(3) \qquad x + y \equiv 0 \pmod 7$$

Даље, из (1) добијамо да је $x - y = n^2 - m^2$ и како је $n^2 - m^2 \equiv 0 \pmod{7^2}$, то је

$$(4) \qquad x - y \equiv 0 \pmod 7$$

Из (3) и (4) сада имамо да је $x + y = 7k$ и $x - y = 7l$, где су $k, l \in N$. Отуда је:

$$2x = 7(k + l), \quad 2y = 7(k - l),$$

где су $k+l$ и $k-l$ природни бројеви, па $7 \mid 2x$ и $7 \mid 2y$, одакле коначно добијамо $7 \mid x$ и $7 \mid y$.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

89

Нека је $(a, m) = 1$ и $b \equiv c \pmod{\varphi(m)}$. Доказати да је тада $a^b \equiv a^c \pmod{m}$.

Доказ. На основу Ојлерове теореме је $a^{\varphi(m)} \equiv 1 \pmod{m}$. Према услову задатка је $b = c + q \cdot \varphi(m)$ за неки цео број q. Зато је $a^{c+q\cdot\varphi(m)} \equiv a^c \pmod{m}$, тј. $a^b \equiv a^c \pmod{m}$. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

90

Ако су p, q различити прости бројеви, доказати да је

$$p^{q-1} + q^{p-1} \equiv 1 \ (mod \ pq).$$

Доказ. Према Малој Фермаовој теореми је

$$p^{q-1} \equiv 1 \pmod{q}$$

и

$$q^{p-1} \equiv 1 \pmod{p},$$

јер је $(p, q) = 1$.
Дакле, $p \mid q^{p-1} - 1$, па и $p \mid p^{q-1} + q^{p-1} - 1$; и $q \mid p^{q-1} - 1$, па и $q \mid p^{q-1} + q^{p-1} - 1$.
Како је $(p, q) = 1$, то $pq \mid p^{q-1} + q^{p-1} - 1$. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

91

Одредити последње три цифре збира бројева:

$$1^{2012} + 2^{2012} + ... + 1000^{2012}.$$

Доказ. Последње три цифре представљају остатак при дељењу броја са 1000. Очигледно је $1000^{2011} \equiv 0 \pmod{1000}$ и $500^{2011} \equiv 0 \pmod{1000}$.
Даље је $999^{2011} \equiv (-1)^{2011} = -1^{2011} \pmod{1000}$.
$998^{2011} \equiv (-2)^{2011} = -2^{2011} \pmod{1000}$;
Уопштено $(1000 - k)^{2011} \equiv (-k)^{2011} = -k^{2011} \pmod{1000} (k \in N \text{ и } k < 1000)$.
Значи да је $1^{2011} + ... + 499^{2011} + 500^{2011} + 501^{2011} + ... + 998^{2011} + 999^{2011} + 1000^{2011} \equiv$

$1^{2011} + 2^{2011} + ... + 499^{2011} + 0 - 499^{2011} - ... - 2^{2011} - 1^{2011} + 0 = 0 \pmod{1000}$.
То значи да је троцифрени завршетак 000.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`https://violetakostadinovic.wordpress.com/iii6-diskretna-matematika/`

92

Одредити остатак при дељењу броја 2^{p^2} са 13, ако се зна да је p прост број већи од 3.

Доказ. Ако је p прост број и $p > 3$, онда је p облика $6k - 1$ или $6k + 1 (k \in N)$.

Како је $(6k \pm 1)^2 = 36k^2 \pm 12k + 1$, то значи да p^2 при дељењу са 12 даје остатак 1 .
Како је $2^{12} = (2^6)^2 = (64)^2 \equiv (-1)^2 = 1 \ (mod \ 13)$то је $2^{p^2} = 2^{12m+1} = (2^{12})^m \cdot 2 \equiv 1^m \cdot 2 = 2 \pmod{13}$.
Дакле, остатак је 2.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`https://violetakostadinovic.wordpress.com/iii6-diskretna-matematika/`

93

Наћи остатак при дијељењу броја $25^{100} + 11^{500}$ са 3.

Доказ. Како је

$$25 \equiv 1 \pmod{3} \text{ и } 11 \equiv -1 \pmod{3} \Rightarrow$$

$$\Rightarrow 25^{100} \equiv 1^{100} \pmod{3} \text{ и } 11^{500} \equiv -1^{500} \pmod{3}.$$

Па добијамо

$$25^{100} \equiv 1 \pmod{3} \text{ и } 11^{500} \equiv 1 \pmod{3}$$

Сабирањем ових бројева $25^{100} + 11^{500} \equiv 2 \pmod{3}$, добијамо као остатак број 2. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`http://www.math.toronto.edu/rosent/Mat246Y/PDF/cong.pdf`

94

Наћи остатак при дијељењу броја:

а) 3^{5555} са 80 б) $3^{100} + 3$ са 28.

Доказ. а) Како је $3^4 = 81 \equiv 1 \pmod{80}$ и $5555 = 4 \cdot 1388 + 3$ Па добијамо:

$$(3^4)^{1388} \equiv 1 \pmod{80}$$

Сабирањем ових конгруенција

$$(3^4)^{1388} \cdot 3^3 \equiv 3^3 \pmod{80}$$

добијамо:

$$3^{5555} \equiv 27 \pmod{80}$$

б) Знамо да је $3^3 = 27 \equiv -1 \pmod{28}$. Даље имамо да је: $1000 = 3 \cdot 333 + 1$
Затим

$$\begin{aligned} (3^3)^{333} &\equiv (-1)^{333} \equiv -1 \pmod{28} \\ 3^{100} = (3^3)^{333} \cdot 3 &\equiv -1 \cdot 3 \equiv -3 \pmod{28} \end{aligned}$$

Такође знамо и да $3 \equiv 3 \pmod{28}$. Па сабирањем ове двије конгруенције добијамо 0.
Што значи да $28 \mid 3^{100} + 3$. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`http://www.math.toronto.edu/rosent/Mat246Y/PDF/cong.pdf`

95

Наћи остатак при дијељењу броја 24^{1947} са 17.

Доказ. Како је $24 \equiv 7 \pmod{17} \Rightarrow 24^{1947} \equiv 7^{1947} \pmod{17}$
И како је 17 прост број и $7 \nmid 17$ по Мала Фермаовој теореми $\Rightarrow 7^{16} \equiv 1 \pmod{17}$.
Па имамо:

$$\begin{aligned} 1947 &= 121 \cdot 16 + 11 \\ (7^{16})^{121} &\equiv 1^{121} \pmod{17} \\ 7^{16 \cdot 121} &\equiv 1 \pmod{17} \\ 7^{16 \cdot 121} \cdot 7^{11} &\equiv 7^{11} \pmod{17} \\ 7^2 &\equiv 15 \pmod{17} \\ 7^2 &\equiv -2 \pmod{17} \\ (7^2)^5 &\equiv (-2)^5 \pmod{17} \\ -32 &\equiv 2 \pmod{17} \\ (7^2)^5 \cdot 7 &\equiv 2 \cdot 7 \equiv 14 \pmod{17} \\ 7^{11} &\equiv 14 \pmod{17} \end{aligned}$$

Па је $24^{1947} \equiv 14 \pmod{17}$.

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`http://repository.sustech.edu/handle/123456789/9301?show=full`

96

Наћи остатак при дијељењу квадрата непарног цијелог броја са 8.

Доказ. За сваки природан број n је

$$(2n+1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1$$

Па пошто $8 \mid 4n(n+1)$ (јер $2 \mid n(n+1)$), то је остатак при дијељењу $(2n+1)^2$ са 8 једнак 1, тј. $(2n+1)^2 \equiv 1 \pmod 8$ □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге TEORIJA BROJEVA:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

97

Доказати да:

а) $27 \mid 2^{5n+1} + 5^{n+2}$ б) $7 \mid 3^{2n+1} + 2^{n+2}$.

Доказ. а) Како је $2^{5n+1} = 2 \cdot 2^{5n}$ и $5^{n+2} = 25 \cdot 5^n$ Па добијамо:

$$\begin{gathered} 2^5 = 32 \equiv 5 \pmod{27} \\ (2^5)^n \equiv 5^n \pmod{27} \\ 2 \cdot (2^5)^n \equiv 2 \cdot 5^n \pmod{27} \end{gathered}$$

Па је

$$2^{5n+1} + 5^{n+2} \equiv 2 \cdot 5^n + 25 \cdot 5^n \pmod{27} \equiv 27 \cdot 5^n \pmod{27} \equiv 0 \pmod{27}$$

б) Знамо да је: $3^{2n+1} + 2^{n+2} = 3 \cdot (3^2)^n + 4 \cdot 2^n$
Па је

$$\begin{aligned} 3^{2n+1} + 2^{n+2} &\equiv 3 \cdot 2^n + 4 \cdot 2^n \pmod 7 \\ 3^{2n+1} + 2^{n+2} &\equiv 7 \cdot 2^n \pmod 7 \\ 3^{2n+1} + 2^{n+2} &\equiv 0 \pmod 7 \end{aligned}$$

Чиме је доказ завршен. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`https://www.math.stonybrook.edu/~olga/mat311-spr09/mat311soln4.pdf`

98

Доказати следећи критеријум дијељивости са бројем 11: природан број је дијељив са 11 ако и само ако му је разлика збира цифара на парним и збира цифара на непарним позицијама дијељива са 11.

Доказ. Узмимо неки природан број и запишимо га као:

$$n = \overline{a_k a_{k-1} ... a_k a_0} = a_k \cdot 10^k + a_{k_1} \cdot 10^{k-1} + ... + a_1 \cdot 10 + a_0$$

гдје су $a_k, ..., a_0$ цифре броја n. Уочимо да вриједи $10 \equiv -1(mod 11)$, па је $10^m \equiv -1(mod 11)$ за непаран m и $10^m \equiv 1(mod 11)$ за паран m. Зато имамо:

$$\begin{aligned} n &\equiv a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + a_4 \cdot 10^4 + a_5 \cdot 10^5 + ...(mod 11) \\ &\equiv a_0 + a_1 \cdot (-1) + a_2 \cdot 1 + a_3 \cdot (-1) + a_4 \cdot 1 + a_5 \cdot (-1) + ...(mod 11) \\ &\equiv (a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)(mod 11) \end{aligned}$$

Одавде следи наведени критеријум; заправо можемо закључити и нешто више: остатак при дијељењу парног броја са бројем 11 једнак је остатку при дијељењу разлике збира његових цифара на парним и непарним мјестима бројем 11 □

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://mnm.hr/wp-content/uploads/2015/10/kongruencije.pdf`

99

Ријешити конгруенцију: $5x \equiv 1 \pmod{12}$

Доказ. Знамо да је нзд$(5, 12) = 1$, тако да нека линеарна комбинација 5 и 12 мора бити једнака 1. Посматрањем утврђујемо да је
$1 = 5 \cdot 5|(-2)$
То значи да су обије стране ове једначине конгруентне једна другој по 12. Слиједи да је:
$1 \equiv 5 \cdot 5 + (-2) \cdot 12 \equiv 5 \cdot 5 \pmod{12}$
Према томе, једно ријешење је $x = 5$.
Да генерализујемо, ако је $x \equiv 5 \pmod{12}$ онда је $5x \equiv 25 \equiv 1 mod 12$

Постоји још један приступ: Почевши од једначине $5x \equiv \pmod{12}$. Када би постојала једнакост, ова једначина би се могла подијелити са 5 да би се добило $x = 1/5$. Међутим дозвољено је да користимо само цијеле бројеве па ово није могуће. Умијесто тога множимо са 5 и добијамо $25x \equiv 5 \pmod{12}$ односно $x \equiv 5 \pmod{12}$. Уочите да ако помножимо са 5 добијамо коефицијент од 1: $5 \cdot 5 \equiv 1 \pmod{12}$ □

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.math.nyu.edu/faculty/hausner/congruence.pdf`

100

Пронаћи $17^{341} \pmod{5}$.

Доказ. Знамо да је

$$17 \equiv 2 \pmod 5$$

Када квадрирамо добијамо

$$17^2 \equiv 4 \equiv -1 \pmod 5$$

Поново квадрирамо

$$17^4 \equiv 1 \pmod 5$$

Знамо да је 1 степеновано на било који број је 1, зато последњу конгруенцију можемо степеновати са 85. Тада имамо

$$17^{340} \equiv 1 \pmod 5$$

На послетку, помножимо са првом конгруенцијом да би добили

$$17^{341} \equiv 2 \pmod 5$$

Дакле остатак је 2.

Идеја је да се нађе неки степен броја 17 да би био $1 \pmod 5$. У овом случају то је било степеновање бројем 4. Затим смо подијелили 341 са 4 и добили коефицијент 85 остатак тог дијељења је 1, затим је коефицијент 85 коришћен у конгруенцији $17^4 \equiv 1 \pmod 5$

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.math.nyu.edu/faculty/hausner/congruence.pdf`

101

Ријешити конгруенцију $8x \equiv 13 \pmod{29}$

Доказ. У аналогији са алгебром очекујемо ријешење

$$x \equiv 13 \cdot 8^{-1} \pmod{29}.$$

Зато прво рачунамо $8^{-1} \pmod{29}$. Изразимо 1 као линеарку комбинацију 8 и 29:

$$1 = 11 \cdot 8 - 3 \cdot 29$$

користећи ово $\pmod{29}$, налазимо $8^{-1} \pmod{29}$. Дакле, ријешавамо по x:

$$x \equiv 13 \cdot 8^{-1} \equiv 13 \cdot 11 = 143 \equiv 27 \pmod{29}$$

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.math.nyu.edu/faculty/hausner/congruence.pdf`

102

Одредити сва ријешења једначине $40y - 63x = 521$ ако су x и y цијели бројеви.

Доказ. Како је $(40, 63) = 1$, једначина увијек има цијелобројна ријешења

$$\begin{aligned} 40y - 63x &= 521 \\ 40y &= 63x + 521 \\ y &= \frac{63x + 521}{40} \\ y &= \frac{80x + 520 - 17x + 1}{40} \\ y &= 2x + 13 - \frac{17x - 1}{40} \end{aligned}$$

да би y био цијели број, онда и $\dfrac{17x - 1}{40} = a$ мора бити цијели број.

$$\begin{aligned} \frac{17x - 1}{40} &= a \\ 17x - 1 &= 40a \\ x &= \frac{40a + 1}{17} \\ x &= \frac{34a + 6a + 1}{17} \\ x &= 2a + \tfrac{6a+1}{17} \end{aligned}$$

да би x био цијели број онда и $\dfrac{6a - 1}{17} = b$, мора бити цијели број.

$$\begin{aligned} \frac{6a - 1}{17} &= b \\ a &= \frac{17b - 1}{6} \\ a &= \frac{18b - b - 1}{6} \\ a &= 3b - \frac{b + 1}{6} \end{aligned}$$

да би a био цијели број онда и $\dfrac{b + 1}{6} = k$, мора бити цијели број

$$\begin{aligned} b + 1 &= 6k \\ b &= 6k - 1 \end{aligned}$$

Тада је:

$$\begin{aligned} a &= \frac{17(6k - 1) - 1}{6} \\ a &= 17k - 3 \end{aligned}$$

Пошто је:

$$x = \frac{40a + 1}{17}$$
$$x = \frac{40(17k - 3) + 1}{17}$$
$$x = 40k - 7$$

Пошто је:

$$y = \frac{63x + 521}{40}$$
$$y = \frac{63(40k - 7) + 521}{40}$$
$$y = 63k + 2$$

Ријешење ове једначине је уређени пар $(x, y) = (40k - 7; 63k + 2)$ □

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`http://www.naukamladima.com/uploads/images/ZadaciPDF/Prijemni%20iz%20matematike%20VIII%20razred/Diofantove%20jednacine/2.pdf`

103

Којом цифром се завршава број 7^{2006}?

Доказ. За рјешавање овог проблема користићемо се чињеницом да последња цифра неког броја је у ствари остатак при дијељењу ток броја са бројем 10.

$$7^2 = 49 \equiv -1(\mod 10)$$

$$7^{2006} = (7^2)^{1003} \equiv (-1)^{1003} = -1(\mod 10)$$

Како је $9 \equiv -1(\mod 10)$, а $0 \leq 9 < 10$, значи да је последња цифра броја 7^{2006} цифра 9. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

104

Доказати да је број дјељив са 9 ако је збир његових цифара дјељив са 9 .

Доказ. Узећемо неки број m , тако да има децимални приказ овог типа :

$$m = c_n 10^n + c_{n-1} 10^{n-1} + ... + c_0$$

Ако посматрамо полином :

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + ... + c_0$$

тако да је f(x) = m. Збир цифара броја m је $c_0 + c_1 + \cdots + c_n$,тј f(1).
како је :

$$10 \equiv 1(\mod 9)$$

слиједи и да је :

$$f(10) \equiv f(1)(\mod 9)$$

Одакле слиједи да су оба броја и f(10) и f(1) истовремено или дјељиви са 9 или нијесу. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

105

Три дата цела броја су потпуни квадрати. Ако је збир та три броја дељив са 9, онда се међу њима могу изабрати два чија је разлика дељива са 9. Доказати.

Доказ. Могући остаци при дељењу квадрата целог броја са 9 су: 0, 1, 4, 7. Нека су x, y и z цели бројеви такви да $9|x^2 + y^2 + z^2$. Претпоставимо да не постоје два броја од x^2, y^2, z^2 која дају исти остатак при дељењу са 9. Тада постоје следеће могућности:
1. Ако је $x^2 \equiv 0(mod 9), y^2 \equiv 1(mod 9), z^2 \equiv 4(mod 9)$, тада је

$$x^2 + y^2 + z^2 \equiv 5(mod 9),$$

што је немогуће јер $9 \mid x^2 + y^2 + z^2$. Исти резулатат се добија ако претпоставимо да је $x^2 \equiv 0(mod 9), z^2 \equiv 1(mod 9), y^2 \equiv 4(mod 9)$ или $y^2 \equiv 0(mod 9), z^2 \equiv 1(mod 9), x^2 \equiv 4(mod 9)$, ...па те случајеве не треба разматрати.
2. Ако је $x^2 \equiv 0(mod 9), y^2 \equiv 4(mod 9), z^2 \equiv 7(mod 9)$, тада је

$$x^2 + y^2 + z^2 \equiv 2(mod 9),$$

што је опет немогуће јер $9 \mid x^2 + y^2 + z^2$.
3. Ако је $x^2 \equiv 1(mod 9), y^2 \equiv 4(mod 9), z^2 \equiv 7(mod 9)$, тада је

$$x^2 + y^2 + z^2 \equiv 3(mod 9),$$

што је такође немогуће јер $9 \mid x^2 + y^2 + z^2$.
4. Ако је $x^2 \equiv 0(mod 9), y^2 \equiv 1(mod 9), z^2 \equiv 7(mod 9)$, тада је

$$x^2 + y^2 + z^2 \equiv 8(mod 9),$$

што је такође немогуће јер $9 \mid x^2 + y^2 + z^2$.

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

106

Дато је једанаест различитих природних бројева. Доказати да међу њима постоји шест бројева чији је збир дељив са 6.

Доказ. Изаберимо било којих пет од једанаест датих бројева.
Међу њима можемо изабрати три броја тако да је њихов збир дељив са 3. На тај начин од тих једанаест бројева можемо изабрати три групе по три броја тако да је у свакој групи збир бројева дељив са 3.
Сада, од те три групе постоје две, такве да су збирови њихових елемената исте парности, па је збир тих шест бројева дељив са 6. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

107

Који је први број у низу:
3, 34, 343, 3 434, 34 343, 343 434, ...
који је дељив са 198?

Доказ. Пошто је $198 = 2 \cdot 3^2 \cdot 11$, тражени број мора бити дељив са 2, па се мора завршавати са 4, тј. облика је

$$343434 \ldots 34 = 2k \text{цифара}$$

Да би био дељив са 9, збир цифара мора да буде дељив са 9, тј. $3k + 4k = 7k$ мора бити дељив са 9, па је $k = 9l$.
Поред тога, да би био дељив са 11 разлика цифара на парним и непарним местима мора бити дељива са 11, тј. $4k - 3k = k$ мора бити дељиво са 11, па је $k = 11m$. Најмањи број који задовољава наведене услове је $k = 9 \cdot 11 = 99$, па тражени број има 198 цифара и налази се на 198. месту у низу. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

108

Одредите све троцифрене природне бројеве који су дјељиви са 7, а при дијељењу с 9 дају остатак 5.

Доказ. Треба одредити све $x = abc = 100a + 10b + c, a, , b, c \in \{0, 1, \ldots, 9\}, a \neq 0$ такве да је

$$x \equiv 0(mod7), x \equiv 5(mod9).$$

Претходни састав конгруенција испуњава услове Кинеског теорема о остатцима и закључујемо да има јединствено рјешење модуло 63. Сва рјешења друге конгруенција у саставу ненегатвних остатака модуло 63 су

$$5,\ 14,\ 23,\ 32,\ 41,\ 50,\ 59$$

а једини међу њима дјељив са 7 је 14 па је

$$x \equiv 14(mod63).$$

Сада још треба одредити све троцифрене бројеве који су конгруентни 14 модуло 63, тј. све $n \in N$ такве да је $n = 63 \cdot k + 14$ и $100 \leq n \leq 999$. Одатле је

$$1.3 < \frac{86}{63} \leq k \leq \frac{985}{63} < 15.7$$

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

109

Нека је n природан број. Докажите да је највећи заједнички дјелилац бројева $n^2 + 1$ и $(n + 1)^2 + 1$ или 1 или 5, те докажите да је једнак 5 ако и само ако је $n \equiv 2 \pmod 5$.

Доказ. Нека је $d = nzd(n^2 + 1, (n + 1)^2 + 1)$. Тада d дијели број

$$((n + 1)^2 + 1) - (n^2 + 1) = 2n + 1,$$

те број

$$n(2n + 1) - 2(n^2 + 1) = n - 2.$$

Према томе, d дијели

$$(2n + 1) - 2(n - 2) = 5,$$

па је $d \in \{1, 5\}$.
Ако број n даје остатке 0,1,2,3,4 при дијељењу с 5, онда број $n^2 + 1$ даје остатке редом 1,2,0,0,2, а $(n + 1)^2 + 1$ остатке редом 2,0,0,2,1. Према томе, бројеви $n^2 + 1$ и $(n + 1)^2 + 1$ истовремено су дјељиви с 5 ако и само ако је $n \equiv 2 \pmod 5$. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view

110

Одредити остатак при дијељењу броја 2^{30} са 13.

Доказ. Како је
$2^{30} = (2^5)^6$, $2^5 = 32 \equiv 6 \pmod{13}$
и
$2^{10} \equiv 6^2 \equiv 10 \pmod{13}$,
то је коначно:
$2^{30} \equiv 10^3 \equiv 12 \pmod{13}$ □

(**Јована Шубарић 11/17 Д**) задатак преузет из књиге MT1003 Pure Mathematics:
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic
pdf

111

Доказати да бројеви a и b имају исте остатке при дељењу са m, само када је $a \equiv b \pmod{m}$.

Доказ. Ако је $a \equiv b \pmod{m}$, тада постоји цео број t такав да је $a = b + mt$. За b и $m \neq 0$ постоје једнозначно одређени цели бројеви q и r такви да је $b = mq + r, 0 \leq r < |m|$, где је r остатак добијен при дељењу b са m. Одавде следи да је $a = m(t+q) + r, 0 \leq r < |m|$. Дакле и број a има исти остатак при дељењу са m
Обратно, нека су a и b бројеви који при дељењу са m имају исте остатке. Тада се може записати да је $a = mg_1 + r$ и $b = mg_2 + r$ при чему је $0 \leq r < |m|$. Одавде следи да је $a - b = m(q1 - q2)$, те је $a \equiv b \pmod{m}$.
С обзиром на доказану теорему релацију конгруенције можемо дефинисати на следећи начин:
Број a је конгруентан броју b по модулу m ако бројеви a и b имају исте остатке при дељењу са $m (m \neq 0)$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic
pdf

112

Наћи последњу цифру броја $1997^{1998^{1999}}$.

Доказ. Нека је $N = 1997^{1998^{1999}}$. Задатак се заправо своди на одређивање $N \pmod{10}$. Како је $1997 \equiv 7 \pmod{10}$, онда је

$$N \pmod{10} \equiv 7^{1998^{1999}}.$$

Са друге стране, из низа $7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$,
$7^3 \equiv 3 \pmod{10}$, $7^4 \equiv 1 \pmod{10}$, $7^5 \equiv 7 \pmod{10}, \ldots$, видимо да је

$$7^a \equiv \begin{cases} 1 \pmod{10} & \text{ако је } a \equiv 0 \pmod{4} \\ 7 \pmod{10} & \text{ако је } a \equiv 1 \pmod{4} \\ 9 \pmod{10} & \text{ако је } a \equiv 2 \pmod{4} \\ 3 \pmod{10} & \text{ако је } a \equiv 3 \pmod{4} \end{cases}$$

Из $1998 \equiv 2 \pmod{4}$, слиједи $1998^{1999} \equiv 2^{1999} \equiv 4 \cdot 2^{1997} \equiv 0 \pmod{4}$, одакле закључујемо да је

$$N \equiv 1 \pmod{10}.$$

□

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`sveska_mat5_(D_smjer)`

113

Доказати да је $11 \cdot 14^n + 1$ сложен број за $n \in \mathbb{N}$.

Доказ. Ако је $N = 11 \cdot 14^n + 1$, покажимо да $p \mid N$ за неки прост број p, такав да је $N > p$.

Ако је $n = 2k$, онда је $14 \equiv -1 \pmod{3}$, одакле је $14^n \equiv 1 \pmod{3}$. Закључујемо да

$$N \equiv 2 \cdot 1 + 1 \equiv 0 \pmod{3},$$

што значи да је дјељив са 3.

У случају да је $n = 2k + 1$, онда је $14 \equiv -1 \pmod{5}$, па је $14^n \equiv -1 \pmod{5}$. Дакле,

$$N \equiv 1 \cdot (-1) + 1 \equiv 0 \pmod{5},$$

чиме је показано да је дјељив са 5.

Значи, у оба случаја закључујемо да је N дјељив са простим бројем који је строго мањи од њега, што значи да је сложен. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic`
`pdf`

114

Ријешимо конгруенцију $555x \equiv 15 \pmod{5005}$

Доказ. Ако скратимо са 5 цијелу конгруенцију, добијамо $111x \equiv 3 \pmod{1001}$. Најприје, рјешавамо конгруенцију

$$111x \equiv 1 \pmod{1001}.$$

Користимо Бланкишип методу

$$\begin{bmatrix} 111 & 1 & 0 \\ 1001 & 0 & 1 \end{bmatrix}$$

Ако помножимо прву врсту са 9 и то одузмемо од друге врсте, добијамо

$$\begin{bmatrix} 111 & 1 & 0 \\ 2 & -9 & 1 \end{bmatrix}$$

Одузимање од прве врсте друге, претходно помножене са 55

$$\begin{bmatrix} 1 & 496 & -55 \\ 2 & -5 & 1 \end{bmatrix}$$

На крају, одузимањем прве врсте од друге, претходно помножене са 2, имамо

$$\begin{bmatrix} 1 & 496 & -55 \\ 0 & x & y \end{bmatrix}$$

Дакле, имамо да је $111 \cdot 496 \equiv 1 \pmod{1001}$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://www.scribd.com/document/341161803/Andrej-Dujella-Uvod-u-Teoriju-Brojeva`

115

Ријешити систем конгруенција

$$x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}, \quad x \equiv 4 \pmod{11}.$$

Доказ. Имамо да је

$$x_0 = 77x_1 + 55x_2 + 35x_3,$$

гдје x_1, x_2, x_3 задовољавају

$$77x_1 \equiv 2 \pmod{5}, \quad 55x_2 \equiv 3 \pmod{7}, \quad 35x_3 \equiv 4 \pmod{11},$$

односно

$$2x_1 \equiv 2 \pmod{5}, \quad 6x_2 \equiv 3 \pmod{7}, \quad 2x_3 \equiv 4 \pmod{11}.$$

Рјешавањем појединачних конгруенција, добијамо

$$x_1 = 1, \; x_2 = 4, \; x_3 = 2,$$

што даје $x_0 = 367$. Према томе, сва рјешења система су дата са

$$x \equiv 367 \pmod{385}.$$

□

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
http://www1.pmf.ni.ac.rs/pmf/predmeti/1083/slike_i_dokumenta/domaci/Domaci_A.pdf

116

Доказати да је број $2^{702} \cdot 19^{826} - 11^{347} \cdot 17^{195}$ дјељив са 3.

Доказ. Задати израз ћемо "разбити"на дјелове па тврђење слиједи из :

$$2 \equiv -1(\mod 3) \Rightarrow 2^{702} \equiv 1(\mod 3);$$

$$19 \equiv 1(\mod 3) \Rightarrow 19^{826} \equiv 1(\mod 3);$$

$$11 \equiv -1(\mod 3) \Rightarrow 11^{347} \equiv -1(\mod 3);$$

$$17 \equiv -1(\mod 3) \Rightarrow 17^{195} \equiv -1(\mod 3);$$

□

(**Милош Ћупић 39/18 Д**) задатак преузет са http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

117

Доказати да је за сваки паран број n број $20^n + 16^n - 3^n - 1$ дјељив са 323.

Доказ. $323 = 17 \cdot 19$. Нека је n произвољан паран број. Из:

$$20 \equiv 3 \pmod{17} \text{ слиједи: } 20^n \equiv 3^n \pmod{17}$$

и из:

$$16 \equiv 3 \pmod{17} \text{ слиједи: } 16^n \equiv 1 \pmod{17}$$

слиједи да $17 \mid 20^n + 16^n - 3^n - 1$.
Такође, из:

$$20 \equiv 1 \pmod{19} \text{ слиједи: } 20^n \equiv 1 \pmod{19}$$

и из:

$$16 \equiv -3 \pmod{19} \text{ слиједи } 16^n \equiv 3^n \pmod{1)9}$$

слиједи да $19 \mid 20^n + 16^n - 3^n - 1$. □

(**Јована Шубарић 11/17 Д**) задатак преузет са `https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic.pdf`

118

Доказати да је број n^2+3n+5није дјељив са 121 ни за један природан број n.

Доказ. Прво ћемо испитати за које n ,$11|n^2+3n+5$
Овдје имамо 11 различитих случајева које требамо да испитамо

$$n \equiv 0(\mod 11) \Rightarrow n^2+3n+5 \equiv 5(\mod 11)$$

$$n \equiv 1(\mod 11) \Rightarrow n^2+3n+5 \equiv 9(\mod 11)$$

$$n \equiv 2(\mod 11) \Rightarrow n^2+3n+5 \equiv 4(\mod 11)$$

$$n \equiv 3(\mod 11) \Rightarrow n^2+3n+5 \equiv 1(\mod 11)$$

$$n \equiv 4(\mod 11) \Rightarrow n^2+3n+5 \equiv 0(\mod 11)$$

$$n \equiv 5(\mod 11) \Rightarrow n^2+3n+5 \equiv 1(\mod 11)$$

$$n \equiv 6(\mod 11) \Rightarrow n^2+3n+5 \equiv 4(\mod 11)$$

$$n \equiv 7(\mod 11) \Rightarrow n^2+3n+5 \equiv 9(\mod 11)$$

$$n \equiv 8(\mod 11) \Rightarrow n^2+3n+5 \equiv 5(\mod 11)$$

$$n \equiv 9(\mod 11) \Rightarrow n^2+3n+5 \equiv 3(\mod 11)$$

$$n \equiv 10(\mod 11) \Rightarrow n^2+3n+5 \equiv 3(\mod 11)$$

Дакле из горе наведених случајева видимо да је једино важи када је $n \equiv 4(\mod 11)$. Дакле :

$$n = 11k + 4, k.jj$$

$$n^2 + 3n + 5 = (11k + 4)^2 + 3(11k + 4) + 5 = 121k(k + 1) + 33$$

Одатле слиједи да $121 \not| n^2 + 3n + 5$
Ако $11 \not| n^2 + 3n + 5$, тада и $121 \not| n^2 + 3n + 5$ □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

119

Доказати да једначина $ax^2 + bx + c = 0$ нема рационалних рјешења ако су a, b, c цијели непарни бројеви.

Доказ. Ово ћемо рјешавати на начин што ћемо претпоставити супротно.
Тада дискриминанта дате квадратне једначине квадрат неког природног броја,
тј. $b^2 - 4ac = k^2$
Како је b^2 непаран број, то је и k^2 непаран број , па је и k непаран број.
У једнакости $b^2 - k^2 = 4ac$, десна страна је дјељива са 4, али не и са 8, јер су a и c непарни бројеви.
Квадрати непарних бројева при дијељењу са 8 дају остатак 1 .
Па је $b^2 - k^2$ дјељиво са 8 - Контрадикција. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

120

Да ли постоји неки природан број који при дељењу са 1001 даје остатак 23, а при дељењу са бројем 1170 остатак 42?

Доказ. Када би постојао природан број n са овим својством, онда би морало да важи:
$n = 1001x + 23$
$n = 1170y + 42$,
тј. $1001x - 1170y = 19$.
Дакле проблем смо свели на решавање ове Диофантове једначине. Уколико она има решења такав број постоји и можемо наћи ког су облика ти бројеви, а уколико једначина нема решења природан број са овим својствима не постоји.
Решење: Проверимо да ли ова Диофантова једначина има решења. Тражимо нзд$(1170, 1001)$:
$1170 = 1001 \cdot 1 + 169$
$1001 = 169 \cdot 5 + 156$

$169 = 156 \cdot 1 + 13$
$156 = 13 \cdot 12$
закључујемо да је нзд$(1170, 1001) = 13$. Како $13 \nmid 19$, следи да једначина нема решења, тј. да не постоји природан број n са овим својствима.
Решење је коректно јер смо задатак свели на решавање Диофантове једначине, а она заиста нема решења уколико нзд$(1170, 1001) \nmid 19$. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

121

Ријешити конгруенцију:
$5x^{99} + x^3 + 2x - 3 \equiv 0 \pmod 5$

Доказ. Како је водећи коефицијент дјељив са 5, дата конгруенција је еквивалентна са:

$$x^3 + 2x - 3 \equiv 0 \pmod 5$$

те има највише 3 рјешења. Пронађимо рјешење:

$$x = 0 : x^3 + 2x - 3 \equiv -3 \pmod 5$$

$$x = 1 : x^3 + 2x - 3 \equiv 0 \pmod 5$$

$$x = 2 : x^3 + 2x - 3 \equiv 4 \pmod 5$$

$$x = 3 : x^3 + 2x - 3 \equiv 0 \pmod 5$$

$$x = 4 : x^3 + 2x - 3 \equiv 4 \pmod 5.$$

Дакле, рјешења полазне конгруенције су:
$x \equiv 1 \pmod 5$
$x \equiv 3 \pmod 5$. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
`https://repozitorij.mathos.hr/islandora/object/mathos%3A260/datastream/PDF/view`

122

Наћи остатак при дјељењу броја 6^{1987} са 37.

Доказ. $6^2 \equiv -1 \pmod{37}$
Тако:
$6^{1987} \equiv 6 \cdot 6^{1986} \equiv 6(6^2)^{993} \equiv 6(-1)^{993} \equiv -6 \equiv 31 \pmod{37}$ □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf

123

Одредити бројеве a и b,тако да је број $n = \overline{a1995} + \overline{1995b}$ дјељив са 44.

Доказ. Како је $44 = 4 \cdot 11$ и $(4, 11) = 1$ закључујемо да број n мора бити дјељив са 4 и са 11. Како је $\overline{a1995} \equiv 3 \pmod 4$ следи да мора бити $\overline{1995b} \equiv 1 \pmod 4$ одакле произилази да је $b \in \{3, 7\}$
Претпоставимо да је најприје b=3.Тада је $19953 \equiv 10 \pmod{11}$,па мора бити да је $\overline{a1995} \equiv 1 \pmod{11}$, одакле следи да је $a + 4 \equiv 1 \pmod{11}$, тј a=8.
Нека је сада b=7 .Слично као у претходном случају закључујемо да мора бити a=4. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/12169/mod_resource/content/1/knjiga_DISKRETNA.pdf

124

Нека је p прост број. Тада конгруенција $x^2 \equiv -1 \pmod p$ има решење ако и само ако је p=2 или $p \equiv 1 \pmod 4$. Доказати.

Доказ. Ако је p=2,тада је x=1 једно решење. Ако је $p \equiv 1 \pmod 4$,тада на основу Вилсонове теореме важи:

$$1 \cdot 2 \cdots \tfrac{p-1}{2} \cdot (p-1)(p-2) \cdots \left(p - \tfrac{p-1}{2}\right) \equiv \left(\left(\tfrac{p-1}{2}\right)!\right)^2 \pmod p \equiv -1 \pmod p$$

па је $x = \frac{p-1}{2}$ једно решење.
Нека је $p \equiv 3 \pmod 4$. Претпоставимо да постоји цио број x,такав да је $x^2 \equiv -1 \pmod p$. Тада је $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$, што је у супротности са Малом-Фермаовом теоремом. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/12169/mod_resource/content/1/knjiga_DISKRETNA.pdf

125

Одредити остатак при дијељењу броја $(7^{2012})^{2014} - (3^{12})^{14}$ са 10.

Доказ. Како је НЗД$(7, 10) = 1$, према Еулеровој теореми слиједи:

$$7^{\varphi(10)} = 7^4 \equiv 1 \pmod{10}$$

Па је:

$$7^{2012} \equiv 1 \pmod{10}$$

Затим слиједи:

$$(7^{2012})^{2014} \equiv 1 \pmod{10}$$

Слично томе:

$$3^{\varphi(10)} = 3^4 \equiv 1 \pmod{10}$$

Одатле слиједи да је:

$$(3^{12})^{14} \equiv 1 \pmod{10}$$

Добили смо да је $(7^{2012})^{2014} - (3^{12})^{14} \equiv 0 \pmod{10}$ што значи да је остатак броја $(7^{2012})^{2014} - (3^{12})^{14}$ при дијељењу са 10 једнак 0. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

126

Одредити остатак при дијељењу броја

$$N_{2017} = 2 + 2^2 + 2^3 + \ldots + 2^{2017}$$

са 127.

Доказ. Важи да је

$$1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 127$$

У збиру N_{2017} сабирке у дисјунктне групе од по седам узастопних сабирака. Збир елемената сваке од тих група задовољава наредне једнакости:

$$2^k + 2^{k+1} + 2^{k+2} + 2^{k+3} + 2^{k+4} + 2^{k+5} + 2^{k+6} = 2^k(1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6) = 2^k \cdot 127.$$

Важи да је $2017 \equiv_7 1$. Поред тога, збир N_{2017} могуће је представити у облику
$N_{2017} = 2 + (2^2 + 2^3 + \ldots + 2^8) + \ldots + (2^{2011} + 2^{2012} + \ldots + 2^{2017})$.
Одатле слиједи да је $N_{2017} \equiv_{127} 2$. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

127

Дато је 2017 узастопних непарних природних бројева $a_1, a_2, \ldots, a_{2017}$. Одредити остатак при дијељењу суме

$$A = a_1 + a_2 + \ldots + a_{2017}$$

са 2017.

Доказ. Нека бројеви a_k, $k = 1, \ldots, 2017$, имају облике

$$a_1 = 2n + 1 = 2n + 2 \cdot 1 - 1$$

$$a_2 = 2n + 3 = 2n + 2 \cdot 2 - 1$$

$$\vdots$$

$$a_{2017} = 2n + 4033 = 2n + 2 \cdot 2017 - 1.$$

У том случају је

$A = a_1 + a_2 + \ldots + a_{2017} = 2017 \cdot 2n + 2(1 + 2 + \ldots + 2017) - (1 + 1 + \ldots + 1) = 2017 \cdot 2n + 2 \cdot \frac{2017 \cdot 2018}{2} - 2017$

$$= 2017(2n + 2017) \equiv_{2017} 0,$$

па је тражени остатак једнак 0. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

128

Одредити последње двије цифре броја $2017^{2016^{2015^{\cdot^{\cdot^{\cdot^{2^1}}}}}}$.

Доказ. Нека је $a = 2017^{2016^{2015^{\cdot^{\cdot^{\cdot^{2^1}}}}}}$ је да важи да је

$$a \equiv_{100} 17^{2017^{2016^{2015^{\cdot^{\cdot^{\cdot^{2^1}}}}}}}.$$

Важе и наредне конгруенције:

$$17^1 \equiv_{100} 17 \quad 17^8 \equiv_{100} 41 \quad 17^{15} \equiv_{100} 93$$

$$17^2 \equiv_{100} 89 \quad 17^9 \equiv_{100} 97 \quad 17^{16} \equiv_{100} 81$$

$$17^3 \equiv_{100} 13 \quad 17^{10} \equiv_{100} 49 \quad 17^{17} \equiv_{100} 77$$

$$17^4 \equiv_{100} 21 \quad 17^{11} \equiv_{100} 33 \quad 17^{18} \equiv_{100} 9$$

$$17^5 \equiv_{100} 57 \quad 17^{12} \equiv_{100} 61 \quad 17^{19} \equiv_{100} 53$$

$$17^6 \equiv_{100} 69 \quad 17^{13} \equiv_{100} 37 \quad 17^{20} \equiv_{100} 1$$

$$17^7 \equiv_{100} 73 \quad 17^{14} \equiv_{100} 29 \quad 17^{21} \equiv_{100} 17$$

На основу претходног јасно слиједи да важи да је $1720k \equiv_{100} 1$ за произвољно $k \in N$. Важи и да је $2016 \equiv_{20} 16$ па је

$$2016^n \equiv_{20} 16^n \equiv_{20} 16,$$

за произвољно $n \in N$, што се једноставно доказује математичком индукцијом, а на основу чињенице да је $16_2 = 256 \equiv_{20} 16 \equiv_{20} 16^1$
Коначно, важи да је

$$a = 2017^{2016^{2015^{\cdot^{\cdot^{\cdot^{2^1}}}}}} = 2017^{2016^{n_0}},$$

gde je $n_0 = 2015^{2014^{\cdot^{\cdot^{\cdot^{2^1}}}}}$ pa se, na osnovu prethodnih rezultata, zaključuje da važi

$$a \equiv 10017^{2016^{\cdot^{\cdot^{\cdot^{2^1}}}}} = 17^{20m_0+16} \equiv 10017^{16} \equiv 10081,$$

na osnovu čega sledi da su poslednje dve cifre broja a cifre 81. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`
(**Лука Брацовић 17/17 Д**) задатак преузет са:
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

129

Одредити све тројке природних бројева (m, n, k) такве да вриједи $3^m + ^n = k^2$.

Доказ. С обзиром да је $7^n = k^2 - 3^m$ слиједи да k^2 и 3^m морају давати исти остатак при дијељењу са 7. а то је могуће ако је m паран број.

$k^2 \equiv 1, 2, 4 \pmod 7$ и $3^m \equiv 1, 2, 4 \pmod 7$ важе само ако је m паран. Дакле, $m = 2l$ важи за неки природан број l, па онда пишемо:

$$7^n = (k - 3^l)(k + 3^l)$$

Из ове једначине слиједи:

$$k - 3^l = 7^a,$$
$$k + 3^l = 7^b$$

гдје су a и b неки ненегативни цијели бројеви за које важи $a < b$. Одузимамо прву једначину од друге и добијамо:

$$2 \cdot 3^l = 7^b - 7^a = 7^a(7^{b-a} - 1)$$

Како $2 \cdot 3^l$ није дјељиво са 7, закључујмо да је $a = 0$ и

$$1 + 2 \cdot 3^l = 7^b$$

За $l = 1$ добијамо да је $m = 2, b = 1$ и $k = 4$, па је онда $n = 1$.

Уколико је $l \geq 2$, онда $7^b = 1 + 2 \cdot 3^l$ даје остатак 1 при дијељењу са 9.

Користећи Еулерову теорему закључујемо да је:

$$7^{\varphi(9)} = 7^6 \equiv 1 \pmod 9$$

За најмањи $d \in N$ такав да је $7^d \equiv 1 \pmod 9$ мора вриједити да $d \mid \varphi(9) = 6$. Стога испитујемо:

$$7^2 \equiv 4 \pmod 9, 7^3 \equiv 1 \pmod 9$$

и добијамо закључак да је $d = 1$, па је $7^{3s} \equiv 1 \pmod 9$ за свако $s \in N$.

Дакле:

$$7^{3s} - 1 = 2 \cdot 3^l$$

за неко $s \in N$. Како је лијева страна претходне једначине дјељива са $7^3 - 1 = 342 = 2 \cdot 3^2 \cdot 19$, тј. са 19, а десна није, закључујемо да за случај $l \geq 2$ нема рјешења.

Тиме добијамо да је једино рјешење: $(m, n, k) = (2, 1, 4)$. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

130

Доказати да 1994 дијели $10^{900} - 2^{1000}$.

Доказ. Број 1994 запишимо у канонском облику:

$$1994 = 2 \cdot 997$$

Како је очигледно да $2 \mid 10^{900} - 2^{1000}$, неопходно је утврдити да ли 997 дијели $10^{900} - 2^{1000}$. Користимо Малу Фермаову теорему и добијамо:

$$10^{996} \equiv 1 \pmod{997}, 2^{996} \equiv 1 \pmod{997}$$

Одатле слиједи да је:

$$2^{1000} \equiv 2^4 = 16 \pmod{997}$$

Као и да је:

$$10^{900} \cdot 10^{96} \equiv 1 \pmod{997}$$

Уочимо да је $10^3 \equiv 3 \pmod{997}$ те је стога:

$$10^{96} \equiv 3^{32} = (3^{16})^2 \equiv 249^2 \equiv 187 \pmod{997}$$

па онда запис:

$$10^{900} \cdot 187 \pmod{997}$$

Узмимо да је $x = 10^{900}$ и ово схватамо као конгруенцију непознате x. Она има рјешење само ако $NZD(187, 997) \mid 1$. Како су 187 и 997 узајамно прости бројеви, овај услов је испуњен. Одатле добијамо да је:

$$x \equiv a \pmod{997}$$

гдје је $\in Z$ такав да је $187a + 997b = 1$.

Бројеве a и b одређујемо проширеним Еуклидовим алгоритмом:

$$997 = 5 \cdot 187 + 62;$$

$$187 = 3 \cdot 62 + 1;$$

$$1 = 187 - 3 \cdot 62;$$

$$1 = 187 - 3 \cdot (997 - 5 \cdot 187);$$

$$1 = 16 \cdot 187 - 3 \cdot 997;$$

Добијамо да је $a = 16, b = -3$. Стога је и:

$$x \equiv 16 \pmod{997}$$

а онда и:

$$10^{900} - 2^{1000} \equiv 16 - 16 = 0 \pmod{997}$$

Овим је доказ завршен. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://tesla.pmf.ni.ac.rs/Dmatem/sem3101/Deljivost%20brojeva.pdf`

131

Доказати да је $9 \cdot 3^{2n} - 8n - 9 \equiv 0 \pmod{64}, n \in N$.

Доказ. Узмимо да је $f(n) = 9 \cdot 3^{2n} - 8n - 9$. Тада је:

$$f(n+1) = 81 \cdot 3^{2n} - 8n - 17;$$

$$f(n+2) = 729 \cdot 3^{2n} - 8n - 25$$

Елиминишемо 3^{2n} из све три једначине и добијамо једначину:

$$f(n+2) - 10f(n+1) + 9f(n) = 64$$

из које следује

$$f(n+2) \equiv 10f(n+1) - 9f(n) \pmod{64}$$

Претпоставимо да је $f(n) \equiv 0 \pmod{64}$ и $f(n+1) \equiv 0 \pmod{64}$. У том случају из последње једнакости важи да је $f(n+2) \equiv 0 \pmod{64}$.

Како је $f(1) = 64 \equiv 0 \pmod{64}$ и $f(2) = 704 \equiv 0 \pmod{64}$, на основу принципа математичке индукције закључујемо да је дато тврђење тачно за све природне бројеве чиме је овај доказ завршен. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://tesla.pmf.ni.ac.rs/Dmatem/sem3101/Deljivost%20brojeva.pdf`

132

Доказати да за непаран број a важи конгруенција $a^{2^n} \equiv 1 (mod 2^{n+2})$ за $n \geq 1$.

Доказ. Доказ изводимо потпуном математичком индукцијом. Ако је $a = 2m - 1$ и $n = 1$ онда је и $a^2 - 1 = 4m(m-1)$.

Овај број је дјељив са $8 = 2^{1+2}$, па тврђење важи за $n = 1$. Претпоставимо да је то тврђење тачно за $n = k$ тј. да је:

$$a^{2^k} \equiv 1 \pmod{2^{k+2}}$$

Како је

$$a^{2^{k+1}} - 1 = a^{2 \cdot 2^k} - 1 = (a^{2^k} - 1)(a^{2^k} + 1)$$

закључујемо да $2^{k+2} \mid a^{2^k} - 1$ по индуктивној хипотези, а $2 \mid a^{2^k} + 1$ јер је a према претпоставци непаран број, па $2^{k+3} \mid a^{2^{k+1}} - 1$.

Тако се доказује да је

$$2^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$$

а то значи да је тврђење тачно и за $n = k + 1$ па самим тим и за свако $n \in N$. □

133

Одредити остатак при дељењу броја 317^{259} са 15.

Доказ. Важи да је $317 = 21 \cdot 15 + 2$, одакле је $317 \equiv 2 \pmod{15}$, па је $317^{259} \equiv 2^{259} \pmod{15}$. Да бисмо нашли остатак при дељењу броја 317^{259} са 15, довољно је наћи остатак при дељењу броја 2^259 са 15.
Важи да је $2^4 = 16 \equiv 1 \pmod{15}$. Како је $259 = 64 \cdot 4 + 3$, то је

$$\begin{aligned} 2^{259} &\equiv (2^4)^6 4 \cdot 2^3 \pmod{15} \\ &\equiv 1^6 4 \cdot 2^3 \pmod{15} \\ &\equiv 8 \pmod{15}. \end{aligned}$$

Како број 2^{259} даје остатак 8 при дељењу са 15, то ће и број 317^{259} такође давати остатак 8 при дељењу са 15, тј. $359^{259} \equiv 8 \pmod{15}$. □

(**Никола Цупара 08/17 Д**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14559/mod_resource/content/1/Kongruencije-peti`
`20termin.pdf`

134

Одредити остатак при дељењу броја 275^{112} са 13.

Доказ. Како је $275 = 21 \cdot 13 + 2$ то је $275 \equiv 2 \pmod{13}$. Довољно је наћи остатак који даје број 2^{112} при дељењу са 13.

$$\begin{aligned} 2 &\equiv 2 \pmod{13} \\ 2^2 &\equiv 4 \pmod{13} \\ 2^3 &\equiv 8 \pmod{13} \\ 2^4 &\equiv 3 \pmod{13} \\ 2^5 &\equiv 6 \pmod{13} \\ 2^6 &\equiv 12 \pmod{13} \\ 2^6 &\equiv -1 \pmod{13} \end{aligned}$$

Како је $112 = 18 \cdot 6 + 4$, то је

$$\begin{aligned} (2^6)^{18} \cdot 2^4 &\equiv (-1)^{18} \cdot 2^4 \pmod{13} \\ 2^{112} &\equiv 16 \pmod{13} \\ 2^{112} &\equiv 3 \pmod{13}. \end{aligned}$$

Па је, $275^{112} \equiv 3 \pmod{13}$. □

(**Никола Цупара 08/17 Д**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14559/mod_resource/content/1/Kongruencije-peti`
`20termin.pdf`

135

Доказати да је за сваки паран број n број $20^n+16^n-3^n-1$ дељив са 323.

Доказ. Да бисмо показалии да је неки број дељив са 323 морамо показати да је дељив са 17 и 19, јер је $323 = 17 \cdot 19$.
Покажимо прво дељивост са 17.
Како је $20 \equiv 3 \pmod{17}$, то је $20^n \equiv 3^n \pmod{17}$.
Како је $16 \equiv -1 \pmod{17}$, то је $16^n \equiv (-1)^n \pmod{17}$. Познато је да је n паран број, одакле је $16^n \equiv 1 \pmod{17}$.
Дакле,

$$\begin{aligned} 20^n + 16^n - 3^n - 1 &\equiv 3^n + 1 - 3^n - 1 \pmod{17} \\ &\equiv 0 \pmod{17}. \end{aligned}$$

Сада покажимо дјељивост са 19.
На исти начин је $20 \equiv 1 \pmod{19}$, одакле је $20^n \equiv 1^n \pmod{19}$, односно $20^n \equiv 1 \pmod{19}$. Аналогно, $16 \equiv -3 \pmod{19}$, одакле је $16^n \equiv (-3^n) \pmod{19}$, због парности броја n следи да је $16^n \equiv 3^n \pmod{19}$. Дакле,

$$\begin{aligned} 20^n + 16^n - 3^n - 1 &\equiv 1 + 3^n - 3^n - 1 \pmod{19} \\ &\equiv 0 \pmod{19}. \end{aligned}$$

С обзиром да су бројеви 17 и 19 узајамно прости, то је $20^n + 16^n - 3^n - 1 \equiv 0 \pmod{17 \cdot 19}$, односно $20^n + 16^n - 3^n - 1 \equiv 0 \pmod{323}$, тј. $323 | 20^n + 16^n - 3^n - 1$.

□

(**Никола Цупара 08/17 Д**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14559/mod_resource/content/1/Kongruencije-peti20termin.pdf`

136

Одредити последњу цифру у декадном запису броја 3^{400}.

Доказ. Треба да одредимо остатак при дељењу броја 3^{400} са 10, јер дељењем неког броја са 10 остатак представља последњу цифру тог броја. Дакле, $3^{400} \equiv ? \pmod{10}$. Имамо:

$$\begin{aligned} 3 &= 3 \pmod{10} \\ 3^2 &= -1 \pmod{10} \\ (3^2)^{200} &= (-1)^{200} \pmod{10} \\ 3^{400} &= 1 \pmod{10} \end{aligned}$$

Дакле, последња цифра броја 3^{400} је 1. □

(**Никола Цупара 08/17 Д**) задатак преузет са
https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%20%28drugi%20deo%29.pdf

137

Наћи остатак при дељењу $(3^{10})^5$ са 35.

Доказ. Како је $(3, 35) = 1$, на основу Ојлерове теореме, следи

$$(3^{\phi})^{(35)} \equiv 1 \pmod{35}$$

$$\phi(35) = \phi(7) \cdot \phi(5) = 6 \cdot 4 = 24$$

$$10^5 = 10000 = 24 \cdot 4166 + 16,$$

одавде следи

$$(3^{10})^5 \equiv (3^{24})^4 166 \cdot 3^{16} \pmod{35}.$$

Како је

$$3^{24} \equiv 1 \pmod{35} \Rightarrow (3^{10})^5 \equiv 3^{16} \pmod{35}$$

$$3^4 \equiv 1 \pmod{35} \Rightarrow 3^{16} \equiv 11^4 \pmod{35}$$

$$11^2 \equiv 16 \pmod{35} \Rightarrow 11^4 \equiv 16^2 \pmod{35}$$

$$16^2 \equiv 11 \pmod{35}.$$

Дакле, остатак је 11. □

(**Никола Цупара 08/17 Д**) задатак преузет са
http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1

138

Дата је конгруенција $5x \equiv 6 \pmod{8}$. Наћи x.

Доказ. Дакле, треба да нађемо x које ће задовољити дату конгруенцију, што значи да треба да нађемо број који када се помножи са 5 и подијели са 8 даје остатак 6.

Да бисмо нашли тај број, кренућемо од $x = 1$ и повећавати редом за по један, док не пронађемо одговарајуће рјешење. Па имамо:

1) $x = 1 - 5 \cdot 1 \equiv 5 \pmod 8 \implies$ није рјешење
2) $x = 2 - 5 \cdot 2 \equiv 10 \pmod 8 \implies 10 \equiv 2 \pmod 8 \implies$ није рјешење

(...)

Прескочићемо остале кораке и прећи одмах на посљедњи.
6) $x = 6 - 5 \cdot 6 \equiv 30 \pmod 8 \implies 30 \equiv 6 \pmod 8 \implies$ ово рјешење задовољава наш услов

Значи, тражено рјешење је $x = \mathbf{6}$.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf`

139

Наћи посљедњу цифру броја 7^{100}.

Доказ. Како тражимо посљедњу цифру броја записаног у декадном бројном систему, то значи да у ствари тражимо остатак овог броја по *модулу* 10.
Означимо тражену цифру са x. Тада имамо:

$$7^{100} \equiv x \pmod{10}$$

Узмимо сада основу 7. Како је $7 \equiv 7 \pmod{10}$, ту не можемо ништа да урадимо. Али, 7^{100} можемо записати као $7^{2^{50}}$, а $7^2 = 49$. Из тога имамо:

$$49 \equiv 9 \pmod{10}$$

Па је:

$$49^{50} \equiv 9^{50} \pmod{10}$$

Сада са 9 поновимо исто што и са 7, односно 9^{50} можемо записати као $9^{2^{25}}$, а $9^2 = 81$. Па имамо:

$$81 \equiv 1 \pmod{10}$$
$$81^{25} \equiv 1^{25} \pmod{10}$$

Како је $1^{25} = 1$, то значи да је:

$$7^{100} \equiv 1 \pmod{10}$$

Из овога имамо да је наша тражена цифра број **1**.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf`

140

Госпођа Валтер је дала испит математичком одјељењу од 5 ученика. Резултате је уносила насумичним редосљедом и након сваког уноса рачунала просјек одјељења. Тада је примијетила да након сваког уноса, просјек је цијели број. Резултати поређани у растућем поретку су: 71, 76, 80, 82, 91. Који је посљедњи резултат који је госпођа Валтер унијела?

Доказ. Да би просјек поступно био цијели број треба нпр. да збир прва 3 резултата буде дјељив са 3, збир прва 4 резултата буде дјељив са 4 итд.
Нађимо остатке свих ових бројева при дијељењу са 3:

$$71 \equiv 2 \pmod 3$$

$$76 \equiv 1 \pmod 3$$

$$80 \equiv 2 \pmod 3$$

$$82 \equiv 1 \pmod 3$$

$$91 \equiv 1 \pmod 3$$

Дакле, остаци су редом: 2, 1, 2, 1, 1. Како збир првих 3 мора да буде дјељив са 3, то значи да збир ових њихових остатака мора да буде дјељив са три. Из ове листе видимо да то је могуће само када саберемо $1 + 1 + 1$, односно да су тражени бројеви: 76, 82 и 91.

$$(76 + 82 + 91) \equiv (1 + 1 + 1) \pmod 3$$

$$(76 + 82 + 91) \equiv 3 \pmod 3$$

$$3 \equiv 0 \pmod 3$$

Остају нам бројеви 71 и 80. Сада тражимо четврти број у низу. Како је збир првих 3 непаран, а збир привх 4 мора да буде дјељив са 4. Непаран број не може бити дјељив са 4, па то значи да треба у низ да додамо непаран број, а то је 71. И сада имамо:

$$71 \equiv 3 \pmod 4$$

$$76 \equiv 0 \pmod 3$$

$$82 \equiv 2 \pmod 3$$

$$91 \equiv 3 \pmod 3$$

$$(76 + 82 + 91 + 71) \equiv (3 + 0 + 2 + 3) \pmod 4$$

$$(76 + 82 + 91 + 71) \equiv 8 \pmod 4$$

$$8 \equiv 0 \pmod 4$$

Кад смо задовољили све претходне услове, остао нам је само један број који је рјешење нашег проблема, а то је **80**.
Посљедњи број који је унијела госпођа Валтер је 80.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf`

141

Наћи колико има цијелих бројева таквих да је $1 \leq n \leq 25$ и $n^2 + 3n + 2$ дјељиво са 6.

Доказ. Ријешимо прво дату квадратну једначину:

$$n^2 + 3n + 2 = 0$$

$$n_{1/2} = \frac{-3 \pm \sqrt{3^2 - 4 \cdot 1 \cdot 2}}{2 \cdot 1}$$

$$n_1 = \frac{-3 + 1}{2} = -1$$

$$n_2 = \frac{-3 - 1}{2} = -2$$

На основу овога наш израз $n^2 + 3n + 2$ можемо записати као $(n + 1)(n + 2)$. То треба да буде дјељиво са 6, односно:

$$(n + 1)(n + 2) \equiv 0 \pmod 6$$

, а то је задовољено само у сљедећим случајевима:

$$2\dot{3} = 6 \equiv 0 \pmod 6$$

$$5\dot{6} = 30 \equiv 0 \pmod 6$$

$$6\dot{1} = 6 \equiv 0 \pmod 6$$

Из овога видимо да је:

$$(n + 1) \equiv 2 \pmod 6$$

$$(n + 1) \equiv 5 \pmod 6$$

$$(n + 1) \equiv 6 \pmod 6$$

, односно:

$$n \equiv 1 \pmod 6$$

$$n \equiv 4 \pmod 6$$

$$n \equiv 5 \pmod 6$$

У опсегу од 1 до 25, бројеви који при дијељењу са 6 дају остатак 1 су: 1, 7, 13, 19 и 25. Остатак 4 дају: 4, 10, 16 и 22. Остатак 5 дају: 5, 11, 17 и 23.
Из овога видимо да првих има 5, других 4 и трећих 4, па је $5 + 4 + 4 = 13$. Што значи да имамо **13**бројева који задовољавају наше услове.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf`

142

Којим цифрама треба замијенити a и b у броју $30a0b03$ да би он био дјељив са 13.

Доказ. Број $30a0b03$ можемо записати на сљедећи начин:

$$30a0b03 = 3000003 + a\dot{1}0000 + b \cdot 100$$

, а у конгруенцији по модулу 13 то је:

$$3000003 + a\dot{1}0000 + b \cdot 100 \equiv 400003 + a \cdot 900 + b \cdot 9 \pmod{13}$$

$$400003 + a \cdot 900 + b \cdot 9 \equiv 10003 + a \cdot (-10) + b \cdot 9 \pmod{13}$$

$$10003 + a \cdot (-10) + b \cdot 9 \equiv 903 + a \cdot 3 + b \cdot 9 \pmod{13}$$

$$903 + a \cdot 3 + b \cdot 9 \equiv (-7) + a \cdot 3 + b \cdot 9 \pmod{13}$$

То даље можемо записати овако:

$$(-7) + a \cdot 3 + b \cdot 9 = 3a + 9b - 7$$

Наставимо даље са конгруенцијом:

$$3a + 9b - 7 \equiv 0 \pmod{13}$$

$$3a + 9b \equiv 7 \pmod{13}$$

Осим 7, ово задовољавају и већи бројеви када на њих додајемо 13, па је:

$$3a + 9b \equiv 20 \pmod{13}$$

$$3a + 9b \equiv 33 \pmod{13}$$

Видимо да у посљедњем случају бројеви 3, 9 и 33 могу да се скрате са 3, а како је нзд$(3, 13) = 1$, можемо све да подијелимо са 3, па имамо:

$$a + 3b \equiv 11 \pmod{13}$$

Да би ово било тачно а и б морају бити:
1) $a = 2$ i $b = 3 \implies 2 + 3 \cdot 3 = 11$
2) $a = 5$ i $b = 2 \implies 5 + 3 \cdot 2 = 11$
3) $a = 8$ i $b = 1 \implies 8 + 3 \cdot 1 = 11$

Из овога имамо да су наша рјешења **(2,3)**, **(5,2)** и **(8,1)**

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf`

143

Нађите остатак при дијељењу броја $3^{100}+5^{100}$ бројем 7.

Доказ. Уочимо да је

$$3^2 \equiv 2 \pmod 7$$

па је

$$3^6 \equiv 2^3 \equiv 1 \pmod 7$$

.

Зато је

$$3^{96} \equiv 1^{16} \equiv 1 \pmod 7$$

,

па је

$$3^{100} \equiv 3^4 \equiv 2^2 \equiv 4 \pmod 7$$

.

Надаље,

$$5 \equiv -2 \pmod 7$$

,

па

$$5^3 \equiv -8 \equiv -1 \pmod 7$$

.

Зато

$$5^{99} \equiv (-1)^{33} \equiv -1 \pmod 7$$

,

а одавде слиједи

$$5^{100} \equiv -5 \equiv 2 \pmod 7$$

.

Коначно,

$$3^{100}+5^{100} \equiv 4+2 \equiv 6 \pmod 7$$

.

□

(**Јакша Мрдак 23/17 Д**) задатак сам смислио.

144

Нађите све природне бројеве m, n који задовољавају једначину 4^m-$9n = 5$.

Доказ. Једначину можемо записати у облику $4^m = 9n + 5$. Одредимо сада све могуће остатке потенције броја 4 при дијељењу бројем 9:

$$4 \equiv 4, 4^4 \equiv 16 \equiv 7, 4^3 \equiv 28 \equiv 1, 4^4 \equiv 4, \cdots \pmod 9$$

Дакле,

$$4^{3k} \equiv 1 \pmod 9$$

,

$$4^{3k+1} \equiv 1 \pmod 9$$

,

$$4^{3k+2} \equiv 1 \pmod 9$$

,

Одавде видимо да не постоји природан број m такав да $4^m \equiv 5 \pmod 9$, па закључујемо како задана једначина нема рјешења у скупу природних бројева.

□

(**Јакша Мрдак 23/17 Д**) задатак сам смислио.

145

Одредити остатак који се добија при дељењу броја 3^{100} бројем 13.

Доказ. Како је:
$3^3 = 27 \equiv 1 \pmod{13}$
$3^{100} = (33)^{33} \cdot 3 \equiv 1 \cdot 3 \pmod{13}$
$3^{100} \equiv 3 \pmod{13}$
Пошто је $0 \leq 3 < 13$, закључујемо да је 3 остатак при дељењу броја 3^{100} бројем 13.

□

(**Јакша Мрдак 23/17 Д**) задатак сам смислио.

146

Којом цифром се завршава број 7^{2006}?

Доказ. Последња цифра неког броја је у ствари остатак при дељењу тог броја бројем 10.

$$7^2 = 49 \equiv -1 \pmod{10}$$

$$7^{2006} = (7^2)^{1003} \equiv (-1)^{1003} = -1 \pmod{10}$$

Како је

$$9 \equiv -1 \pmod{10}$$

,

а

$$0 \leq 9 < 10$$

,

значи да је последња цифра броја 7^{2006} цифра 9

□

(**Јакша Мрдак 23/17 Д**) задатак сам смислио.

147

Доказати да је број дељив са 9 ако је збир његових цифара дељив са 9.

Доказ. Узмимо неки број m, тако да он има децимални приказ:

$$m = c_n 10^n + c_{n-1} 10^{n-1} + \cdots + c_0$$

.

Ако посматрамо полином:

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$$

,

тада је

$$f(10) = m$$

.

Збир цифара броја m је

$$c_0 + c_1 + \cdots + c_n$$

to jest $f(1)$.
Kako je

$$10 \equiv 1 \pmod 9$$

,
slijedi da je i

$$f(10) \equiv f(1) \pmod 9$$

.
Odakle slijedi da su oba broja i $f(10)$ i $f(1)$ istovremeno ili djeljiva sa 9 ili nisu.

□

(**Јакша Мрдак 23/17 Д**) zadatak sam smislio.

148

Одредити остатак који се добија при дијељењу броја $3^{105} + 4^{105}$ са 11

Доказ. Прво ћемо наћи остатак при дијељењу 3^{105} са 11

$$\begin{aligned} 3 &\equiv 3 \pmod{11} \\ 3^2 &\equiv -2 \pmod{11} \\ 3^3 &\equiv -6 \pmod{11} \end{aligned}$$

До претходног закључка можемо доћи на два начина, прво, знамо да броју $3^3 = 27$ фали још 7 до броја 33 који је дјељив са 11. Друго, већ смо показали да је $3 \equiv 3 \pmod{11}$ и $3^2 \equiv -2 \pmod{11}$
одакле је, $3^3 = 3 \cdot 3^2 \equiv 3 \cdot (-2) \pmod{11}$.
Такође можемо рећи и да је

$$3^3 \equiv 5 \pmod{11}$$

На исти начин закључујемо даље

$$\begin{aligned} 3^4 &\equiv 4 \pmod{11} \\ 3^5 &\equiv 1 \pmod{11} \\ (3^5)^{21} &\equiv 1^2 1 \pmod{11} \\ 3^{105} &\equiv 1 \pmod{11} \end{aligned}$$

Сада ћемо наћи остатак при дијељењу броја $4^1 05$ са 11

$$\begin{aligned} 4 &\equiv 4 \pmod{11} \\ 4^2 &\equiv 5 \pmod{11} \\ 4^3 &\equiv -2 \pmod{11} \\ 4^4 &\equiv 3 \pmod{11} \\ 4^5 &\equiv 1 \pmod{11} \\ (4^5)^{21} &\equiv 1^2 1 \pmod{11} \\ 4^{105} &\equiv 1 \pmod{11} \end{aligned}$$

На крају,

$$3^{105} + 4^{105} \equiv 1 + 1 \pmod{11} \equiv 2 \pmod{11}$$

□

(**Филип Станковић 5/17 Д**)
https://cheap-library.com/book/97d53ce53ef2c7df095954048398 76f8

149

Наћи последњу цифру броја 7^{7^7}

Доказ. Како би пронашли последњу цифру броја 7^{7^7}, тражимо његов $\pmod{10}$

$$\begin{aligned} 7^2 &\equiv -1 \pmod{10} \\ 7^3 \equiv 7^2 \cdot 7 &\equiv -7 \equiv 3 \pmod{10} \\ 7^4 \equiv (7^2)^2 &\equiv 1 \pmod{10} \end{aligned}$$

Такође,

$$\begin{aligned} 7^2 &\equiv 1 \pmod{4} \\ 7^7 \equiv (7^2)^3 \cdot 7 &\equiv 3 \pmod{4} \end{aligned}$$

Што значи да постоји број t, такав да $7^7 = 3 + 4t$, и из тога слиједи

$$7^{7^7} \equiv 7^{4t+3} \equiv (7^4)^t \cdot 7^3 \equiv 1^t \cdot 3 \equiv 3 \pmod{10}$$

Значи, заднја цифра је 3

□

(**Филип Станковић 5/17 Д**)

https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf

3 Прости бројеви

150

Доказати да је сваки прост број $p > 3$ облика $6k + 1$ или $6k + 5$.

Доказ. Уочимо да су сви ненегативни цијели бројеви облика:

$$6k,\ 6k+1,\ 6k+2,\ 6k+3,\ 6k+4,\ 6k+5$$

Како су бројеви облика: $6k$, $6k+2$, $6k+4$ парни, можемо закључити да ови бројеви не могу бити прости за неко $p > 3$.
Ако погледамо сада бројеве облика $6k + 3$, јасно је да су то бројеви који су дељиви са 3, односно и бројеви овог облика су сложени.
И заиста, остају само бројеви облика $6k + 1$ и $6k + 5$, међу којима су сви прости бројеви већи од 3. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге MT1003 Pure Mathematics:
`https://cheap-library.com/book/97d53ce53ef2c7df09595404839876f8`

151

Доказати да за било који цијели број $n > 1$ број $n^5 + n^4 + 1$ није прост.

Доказ. Како је:

$$\begin{aligned} n^5 + n^4 + 1 &= n^5 + n^4 + n^3 - n^2 - n + n^2 + n + 1 \\ &= n^3(n^2 + n + 1) - n(n^2 + n + 1) + n^2 + n + 1 \\ &= (n^2 + n + 1)(n^3 - n + 1) \end{aligned}$$

Производ ова два броја већи од 1(у поставци имамо да је $n > 1$), доказали смо да број $n^5 + n^4 + 1$ није прост. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге Number Theory: Structures, Examples, and Problems:
`https://www.springer.com/gp/book/9780817632458`

152

Доказати да су n і $n+1$ релативно прости за свако $n \in N$.

Доказ. Претпоставимо супротно, да нису узајамно прости, односно да је нзд$(n, n+1) = x$, при чему x не може бити 1, односно $x > 1$. Одавде слиједи да $x \mid n$ и $x \mid n+1 \Rightarrow x \mid n+1-n$ Овиме добијамо да $x \mid 1$, а како нема броја који дијели 1 осим $1 \Rightarrow x = 1$. Тако да смо контрадикцијом доказали да су n і $n+1$ релативно прости за свако $n \in N$. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге Number Theory:
`https://artofproblemsolving.com/articles/files/SatoNT.pdf`

153

Доказати да се сваки прост број облика $3k+1$ може приказати у облику броја $6m+1$.

Доказ. Уочимо да је једини паран прост број 2 и он није облика $3k+1$.
Ово значи да је сваки прост број облика $3k+1$ непаран. Из овог слиједи да је број $3k$ паран, што даље имплицира да и k мора бити паран број, односно можемо означити: $k = 2m$.
Тј.

$$3k + 1 = 3(2m) + 1 = 6m + 1$$

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге Elementary Number Theory in Nine Chapters:
`https://www.amazon.com/Elementary-Number-Theory-Nine-Chapters/dp/0521615240`

154

Доказати да простих бројева облика $4k+3$ има бесконачно много за свако $k \in N$.

Доказ. Сви прости бројеви већи од 2 су непарни и облика $4k+1$ или $4k+3$. Производ бројева облика $4k+1$ и сам има тај облик. Заиста,

$$(4a + 1)(4b + 1) = 4(4ab + a + b) + 1$$

Нека су сада $p_1, p_2, \ldots, p_n$ сви прости бројеви облика $4k+3$. Погледајмо сада број

$$N = 4 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1 = 4 \cdot (p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1) + 3$$

Тада је N или прост број, или се може раставити на продукт простих бројева, од којих ниједан није $p_1, ..., p_n$ јер је остатак дијељења броја N са неким од бројева p -1.
Затим, сви прости фактори броја N не могу бити облика $4k+1$, јер N није тог облика. Као што смо видјели, продукт бројева облика $4k+1$ је такође број тог истог облика. Према

томе, бар један прост фактор мора бити облика $4k+3$, што није могуће, јер тај фактор није ниједан од бројева p, за које смо раније претпоставили да су сви прости бројеви облика $4k+3$, па можемо закључити да је број простих бројева облика $4k+3$ бесконачан. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из књиге Equations and Inequalities: Elementary Problems and Theorems in Algebra and Number Theory: `https://www.springer.com/gp/book/9780387989426`

155

Ако су бројеви p и $2p^2+1$ прости, доказати да је и $3p^2+2$ такође прост.

Доказ. Ако је p прост број већи од 3, тада је p облика $6k+1$ или $6k+5$ за неко k. Ако је $p=6k+1$, тада је број

$$2p^2+1=2(6k+1)^2+1=2(36k^2+12k+1)+1=3(24k^2+8k+1)$$

сложен. Ако је $p=6k+5$, тада је опет број

$$2p^2+1=2(6k+5)^2+1=2(36k^2+60k+25)+1=3(24k^2+40k+17)$$

сложен.
Дакле, p је прост број мањи од 5, тј. $p=2$ или $p=3$. Ако је $p=2$, тада је $2p^2+1=9$ сложен број. За $p=3$, $2p^2+1=19$ је прост број, а прост је и $3p^2+2=29$. □

(**Катарина Синђић 36/19 Д**) задатак преузет са `https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf`

156

Доказати да за свако n из скупа природних бројева, број $2^{2^n}+2^{2^{n-1}}+1$ има најмање n различитих простих фактора.

Доказ. Доказаћемо тврђење индукцијом по n.

За $n=1$ је $2^{2^1}+2^{2^0}+1=7$. За сваки реалан број x важи једнакост:

$$x^4+x^2+1=(x^2+1)^2-x^2=(x^2-x+1)(x^2+x+1),$$

па специјално и

$$2^{2^{n+1}}+2^{2^n}+1=(2^{2^n}-2^{2^{n-1}}+1)(2^{2^n}+2^{2^{n-1}}+1).$$

Даље имамо да је $(2^{2^n}-2^{2^{n-1}}+1, 2^{2^n}+2^{2^{n-1}}+1)=1$, јер ако би ови бројеви имали заједнички прост фактор $p>2$ ($p\neq 2$ јер су бројеви непарни), онда би било

$$p \mid (2^{2^n}+2^{2^{n-1}}+1)-(2^{2^n}-2^{2^{n-1}}+1)=2\cdot 2^{2^{n-1}},$$

што је немогуће, јер p је непаран прост број.

Дакле, по претпоставци, ако $2^{2^n}+2^{2^{n-1}}+1$ има најмање n различитих простих дјелилаца, онда $2^{2^{n+1}}+2^{2^n}+1$ има најмање $n+1$ различитих простих дјелилаца. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`https://www.scribd.com/document/317815399/Zbirka-teorija-brojeva`

157

Наћи све природне бројеве n за које је број $[\frac{n^3+8n^2+1}{3n}]$ прост.

Доказ. Ако је $n=3k$, онда је

$$[\frac{n^3+8n^2+1}{3n}]=3k^2+8k=k(3k+8).$$

Он је прост само ако је $k=1$. Тада је $n=3$.

Ако је $n=3k+1$, онда је

$$[\frac{n^3+8n^2+1}{3n}]=(3k+1)(k+3).$$

Он је прост само ако је $k=0$. Тада је $n=1$.

Ако је $n=3k+2$, онда је

$$[\frac{n^3+8n^2+1}{3n}]=3k^2+12k+6=3(k^2+4k+2).$$

сложен број. □

(**Катарина Синђић 36/19 Д**) задатак преузет са `https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf`

158

(а) Доказати да су свака два различита Фермаова броја узајамно проста.
(б) Доказати да Фермаови бројеви задовољавају рекурентну релацију $f_{n+1}=f_0f_1f_2\dots f_n+2$.

Доказ. (а) Бројеви $f_n=2^{2^n}+1$ се називају Фермаови бројеви. Фермат је сматрао да су сви они прости. Заиста, $f_0=3, f_1=5, f_2=17, f_3=257, f_4=65537$ су прости. Нека су f_n и f_{n+k}, при чему је $k>0$, два различита Фермаова броја. Сада претпоставимо да је m цио позитиван број, такав да $m\mid f_n$ и $m\mid f_{n+k}$. Нека је $x=2^{2^n}$, тада је:

$$\frac{f_{n+k}-2}{f_n}=\frac{x^{2^k}-1}{x+1}=x^{2^k-1}-x^{2^k-2}+\dots-1,$$

па $f_n \mid f_{n+k} - 2$, одакле слиједи да $m \mid f_{n+k} - 2$. Како $m \mid f_{n+k}$, то $m \mid 2$. Међутим, како су Фермаови борјеви непарни, то слиједи да је $m = 1$. Тиме смо доказали да су свака два различита Фермаова броја узајамно проста.

(б) Ово тврђење ћемо доказати индукцијом по n. За $n = 0$ је $f_0 = 3$, а $f_1 = 5$, па тврђење важи. Сада претпоставимо да тврђење важи за неки природан број n, тј. да је $f_n = f_0 f_1 \dots f_{n-1} + 2$, тада је

$$f_n - 2 = 2^{2^n} + 1 - 2 = 2^{2^n} - 1 = f_0 f_1 \dots f_{n-1},$$

па је даље

$$f_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1) = f_0 f_1 \dots f_{n-1} \cdot f_n,$$

чиме је доказ завршен. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`https://www.docsity.com/sr/prosti-brojevi-vezbe-teorija-brojeva-matematika/361264/`

159

(а) Одредити све просте бројеве p, такве да је $\frac{7}{6} > \frac{5}{p} > \frac{2}{5}$.
(б) Доказати да остатак при дијељењу простог броја са бројем 30 не може бити сложен број.

Доказ. (а) Из задатог односа међу разломцима $\frac{7}{6} > \frac{5}{p} > \frac{2}{5}$, слиједи да је и

$$\frac{5}{2} > \frac{p}{5} > \frac{6}{7}.$$

Сада, да би било лакше поређење, разломке ћемо проширити тако да их доведемо на исте имениоце. нзс$(2, 5, 7) = 70$, што значи да је заједнички одговарајући именилац број 70. Из тога даље слиједи:

$$\frac{175}{70} > \frac{14p}{70} > \frac{60}{70},$$

односно, $175 > 14p > 60$. Одавде је

$$\frac{175}{14} > p > \frac{60}{14}.$$

На тај начин добијамо да је $p = 5, 7, 11$.

(б) Ако би остатак при дијељењу простог броја p са бројем 30 нпр. био 14, тада би било

$$p = 30 \cdot q + 14 = 2(15 \cdot q + 7),$$

па би p био дјељив са 2, што је супротно претпоставци да је прост. На сличан начин би елиминисали све могућности да остатак буде сложен број и добили да важи тврђење задатка. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf

160

(а) Нека је p прост број већи од 2. За $k \in \{1, 2, \dots p-1\}$, нека је r_k остатак при дијељењу броја k^p са p^2. Доказати да је

$$r_1 + r_2 + \dots r_{p-1} = \frac{p^3 - p^2}{2}.$$

(б) Одредити најмањи природан број који има тачно 4 дјелиоца.
(в) Одредити најмањи природан број који је дјељив са 30 и има тачно 12 дјелилаца.

Доказ. (а) За $k \in \{1, 2, \dots p-1\}$, имамо следеће:

$$\begin{aligned} k^p + (p-k)^p &= k^p + p^p - \binom{p}{1} p^{p-1}k + \dots + \binom{p}{p-1} pk^{p-1} - k^p \\ &= p^p - \binom{p}{1} p^{p-1}k + \binom{p}{2} p^{p-2}k^2 + \dots + p^2 k^{p-1}, \end{aligned}$$

па $p^2 \mid k^p + (p-k)^p$, одакле слиједи да $p^2 \mid r_k + r_{p-k}$. Међутим, како је $r_k < p^2$ и $r_{p-k} < p^2$, то је $r_k + r_{p-k} = p^2$. Из тога даље слиједи:

$$\begin{aligned} r_1 + r_2 + \dots + r_{p-1} &= (r_1 + r_{p-1}) + (r_2 + r_{p-2}) + \dots + (r_{\frac{p-1}{2}} + r_{\frac{p+1}{2}}) \\ &= \frac{p-1}{2} p^2 \\ &= \frac{p^3 - p^2}{2}. \end{aligned}$$

Чиме је доказ завршен.

(б) Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ канонска факторизација броја n, тада је $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$, што представља број позитивних дјелилаца броја n. Да бисмо одредили n, потребно је одредити:

- k - број међусобно различитих простих дјелилаца од n
- $p_1, p_2, \dots, p_k$ - просте чиниоце броја n
- $\alpha_1, \alpha_2, \alpha_k$,

тако да је $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ најмањи број са особином

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) = 4$$

Пошто је $\alpha_i + 1 \geq 2, i = 1, 2, \dots, k$ и $4 = 2 \cdot 2$, слиједи да је $k = 2$, тј. да n има само два проста фактора и при томе је:

$$\alpha_1 + 1 = 2 \text{ и } \alpha_2 + 1 = 2$$
$$\Longrightarrow \alpha_1 = 1 \text{ и } \alpha_2 = 1$$

Дакле, n је производ два проста броја ($n = p_1 \cdot p_2$), а најмањи међу њима је производ прва два проста броја ($p_1 = 2$ и $p_2 = 3$). Дакле, $n = 6$.

(в) Нека је n тражени број. Како $30 \mid n$, слиједи да $2 \mid n, 3 \mid n$ и $5 \mid n$. Тада је:

$$n = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma} ... (\alpha, \beta, \gamma \geq 1),$$

па је

$$\tau(n) = (\alpha + 1)(\beta + 1)(\gamma + 1)(...) = 12 = 2 \cdot 2 \cdot 3,$$

одакле се види да број n нема других простих дјелилаца осим 2,3 и 5, тј. да је $2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma}$, као да је и због услова минималности броја n

$$\alpha + 1 = 3, \beta + 1 = 2, \gamma + 1 = 2.$$

Дакле, тражени број је $n = 2^2 \cdot 3 \cdot 5 = 60$. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

161

Наћи све просте бројеве p такве да су и бројеви:
a) $8p^2 + 1$ b) $p + 10$ и $p + 14$ прости.

Доказ. a) Ако је $p = 2$, тада $8p^2 + 1 = 33$ није прост број.
Ако је $p = 3$, тада $8p^2 + 1 = 73$ јесте прост број.
За $p = 5$ број $8p^2 + 1 = 201$ није прост.
Нека је сада p прост број већи од 5. Тада је p облика $6k + 1$ или $6k + 5, (k \in N)$. Ако је $p = 6k + 1$, тада је

$$8(6k + 1)^2 + 1 = 8(36k^2 + 12k + 1) + 1 = 3 \cdot (96k^2 + 32k + 3)$$

сложен број. Ако је $p = 6k + 5$, тада је

$$8(6k + 5)^2 + 1 = 8(36k^2 + 60k + 25) + 1 = 3 \cdot (96k^2 + 160k + 67)$$

сложен број.
Дакле, једино решење је $p = 3$.

b) За $p = 2$ број $p + 10 = 12$ није прост.
За $p = 3$ бројеви $p + 10 = 13$ и $p + 14 = 17$ су прости.
Ако је $p = 5$, тада опет број $p + 10 = 15$ није прост.
Нека је p прост број већи од 5. Могућа су два случаја:

$$p = 6k + 1k - jp + 14 = 6k + 15 = 3(2k + 5)j;$$
$$p = 6k + 5k - jp + 10 = 6k + 15 = 3(2k + 5)j;$$

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

162

Доказати да је сваки број облика $3n - 1$ дјељив са неким простим бројем облика $3k - 1$.

Доказ. Сваки прсот број осим броја 3 или је облика $3k - 1$ или облика $3k + 1$. Ако дати број облика $3n - 1$ нема ни један прост чинилац облика $3k - 1$,онда су сви његови прости чиниоци облика $3k + 1$.Тада је, због $(3k + 1)(3j + 1) = 3(3kj + k + j) + 1$, производ свих простих чинилаца тог облика такође облика $3m + 1$,што није могуће. Дакле, дати број има прост чинилац облика $3k - 1$. □

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

163

Доказати да међу 30 узастопних природних бројева,где је најмањи већи од 5, има највише 8 простих

Доказ. Од тих 30 узастопних бројева 15 је парних,5 оних који су дељиви са 3,а нису дељиви са 2 и још 2 који се дељиви са 5,а нису дељиви ни са 2 ни са 3. Према томе, бар 15+5+2=22 броја су сложена,па простих не може бити више од 8. □

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

164

Ако је p прост број већи од 3 доказати да је $p^2 - 1$ дјељив са 24.

Доказ. С обзиром да је p прост, он је и непаран, па је

$$p^2 - 1 \equiv (p+1)(p-1)$$

производ два парна броја,који су и узастопни парни бројеви.Па је један од њих дјељив са 2,а други са 4,зато је и њихов производ $(p+1)(p-1)$ дјељив са 8. Такође,пошто је p прост број он сигурно није дјељив са 3, а $p+1p-1$ су му претходник и следбеник, од којих је један сигурно дјељив са 3. Па како смо показали да је овај производ дјељив са 8 и са 3,онда је он дјељив и са 24.

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

165

Природан број n има само три проста дјелиоца : 2,3 и 5. Одредити број n ако је :
$\tau(\frac{n}{2}) = \tau(n) - 30$, $\tau(\frac{n}{3}) = \tau(n) - 35$ и $\tau(\frac{n}{5}) = \tau(n) - 42$.

Доказ. Нека је $n = 2^x \cdot 3^y \cdot 5^z$. Тада је:

$$\tau(\frac{n}{2}) = x(y+1)(z+1)$$
$$\tau(\frac{n}{3}) = (x+1)y(z+1)$$
$$\tau(\frac{n}{5}) = (x+1)(y+1)z,$$

па је:

$$\begin{aligned}\tau(n) = (x+1)(y+1)(z+1) &= x(y+1)(z+1) + 30 \\ &= (x+1)y(z+1) + 35 \\ &= (x+1)(y+1)z + 42,\end{aligned}$$

одакле добијамо систем једначина:

$$(y+1)(z+1) = 30$$
$$(x+1)(z+1) = 35$$
$$(x+1)(y+1) = 42.$$

Рјешење овог система је $x = 6$, $y = 5$, $z = 4$, па је $n = 9\ 720\ 000$. □

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

166

а) Ако су p и $8p-1$ прости бројеви, доказати да је $8p+1$ сложен број.

б) Ако су p и $2p+1$ прости бројеви ($p>3$), доказати да је $4p+1$ сложен број.

Доказ. а) Важно је приметити да је тврђење овог дела задатка еквивалентно са:

ако је p прост број, тада је $8p-1$ сложен или је $8p+1$ сложен.

Заиста, ако је q ="број p је прост", r = "број $8p-1$ је прост", s = "број $8p+1$ је прост", тврђење под а) је

$$q \wedge r \Rightarrow \neg s,$$

па пошто је формула $(q \wedge r \Rightarrow \neg s) \Leftrightarrow (q \Rightarrow \neg r \vee \neg s)$ таутологија, тврђење под а) може се формулисати и на следећи начин:

ако је p прост број, тада је бар један од бројева $8p-1$ или $8p+1$ сложен.

За $p=2$ број $8p-1$ није прост. За $p=3$ тврђење очигледно важи.
Свакии прост број $p>3$ је облика $3k-1$ или $3k+1$, за неки природан број k.

Ако је p прост број облика $3k-1$, за неки k, тада је $8p-1 = 24k-9 = 3(8k-3)$ сложен јер је $8k-3>1$ за $k \geqslant 1$.

Ако је p прост број облика $3k+1$, за неки k, тада је $8p+1 = 24k+9 = 3(8k+3)$ сложен јер је $8k+3>1$ за $k \geqslant 1$.

б) Слично као и делу а), довољно је доказати да важи:

ако је p прост број већи од 3, тада је бар један од бројева $2p+1$ или $4p+1$ сложен.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

167

Да ли постоји прост број који се може представити у облику збира кубова два природна броја ?

Доказ. Ако такав прост број p постоји, он би се могао представити као:

$$p = a^3 + b^3$$

где су a и b природни бројеви. Овде нам је неопходно познавање формуле за растав збира кубова : $a^3 + b^3 = (a + b) \cdot (a^2 - ab + b^2)$ Па кад њу искористимо, имали би да је:

$$p = (a + b) \cdot (a^2 - ab + b^2)$$

Пошто прост број нема других чинилаца сем 1 и самог себе, и због чињенице да је $a+b > 1$, имаћемо да је

$$a^2 - ab + b^2 = 1$$

Решимо ову једначину у скупу природних бројева.
Она је еквивалентна са: $2a^2 - 2ab + 2b^2 = 2$. Односно, $a^2 + b^2 + (a - b)^2 = 2$.Одавде добијамо да је једино решење, за нас интересантно, $a = 1$ и $b = 1$,јер је услов да буду природни бројеви (Када би тражили целобројна решења, имали би и парове (1,0) и (0,1)). Па из овога добијамо да постоји прост број $p = 2$ за природне бројеве $a = 1$ и $b = 1$, такав да је $p = 2 = 1^3 + 1^3$.Друге могућности не постоје. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

168

Доказати да за сваки природан број n постоји скуп од n сложених бројева који образују аритметичку прогресију, при чему су ти бројеви по паровима узајамно прости.

Доказ. Ако је $2 \leqslant k \leqslant N$,број $N! + k$ је сложен, За дати природан број n изаберимо прост број p такав да је $p > n$ и цео број $N \geqslant p + (p - 1)n!$. Тада сложени бројеви

$$N! + p, N! + p + n!, \ldots, N! + p + (n - 1)n!$$

образују аритметичку прогресију. Ако је q заједнички прост дјелилац нека два броја горњег низа, онда је и разлика та два броја $jn!(0 < j < n)$ дељива са q. Одатле следи да је $q \leqslant n$. Тада је и $N!$ дељив са q, па према томе и p, што је немогуће. Добијена контрадикција показују да су свака два члана низа узајамно прости бројеви. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са `https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf`

169

Ако је p прост број, доказати да је $\frac{(2p)!}{(p!)^2} - 2$ дељиво са p^2.

Доказ. За свако реално x важи

$$(1+x)^p(1+x)^p = (1+x)^{2p}.$$

Ако развијемо ове изразе по биномној формули и изједначимо коефицијенте уз x^p добијамо

$$\binom{p}{1}\binom{p}{p-1} + \binom{p}{2}\binom{p}{p-2} + \ldots + \binom{p}{p-1}\binom{p}{1} + 1 = \binom{2p}{p},$$

односно

$$N = \frac{(2p)!}{(p!)^2} - 2 = \binom{2p}{p} - 2 = \sum_{i=1}^{p-1}\binom{p}{i}^2.$$

Како је p прост број, то је сваки од бројева

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$$

дељив са p, па је последњи збир, а са њим и број N, дељив са p^2.
Напомена. $\binom{n}{k} = \binom{n}{n-k}$ и $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са `https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf`

170

Нека је $p_n n$-ти прост број ($p_1 = 2, p_2 = 3, p_3 = 5, \ldots$) и нека је $\pi(n)$ број простих бројева који нису већи од n. Ако је

$A = \{n + p_n | n \in N\}$ и $B = \{n + \pi(n) + 1 | n \in N\}$,

тада је $A \cap B = \emptyset, A \cup B = N \setminus \{1\}$. Доказати.

Доказ. Функција π има следећа својства:

(1) $\pi(p_k) = k$ за свако $k \in N$,
(2) $\pi(n) \leqslant \pi(n+1)$ за свако $n \in N$,
(3) $\pi(n) < \pi(n+1)$ ако и само ако је $n+1$ прост број. Претпоставимо супротно,тј. да је $A \cap B \neq \emptyset$,односно да за неке природне бројеве m и n важи

$$(*) \quad m + p_m = n + \pi(n) + 1.$$

Размотрићемо две могућности: $p_m \leqslant n$ и $p_m > n$.
Ако би било $p_m \leqslant n$, тада би из те релације и из

$$m = \pi(p_m) \leqslant \pi(n)$$

следило

$$m + p_m \leqslant n + \pi(n) < n + \pi(n) + 1.$$

што је супторно са (*) Како је у случају $p_m > n, m = \pi(p_m) > \pi(n)$ то је $m \geqslant \pi(n) + 1$ и $m + p_m > n + \pi(n) + 1$, што поново противуречи претпоставци (*).
Тиме је доказано да је $A \cap B = 0$.
Докажимо сада да је $A \cup B = N \setminus \{1\}$. Јасно је да $1 \notin A \cup B$ и да $2 \in B$. Нека је $n > 2$ произвољан природан број који не припада скупу A. Докажимо да тада $n \in B$. Нека за неко $m \in N$ важи

$$m + p_m < n < m + 1 + p_{m+1},$$

тј.

$$p_m \leqslant n - m - 1 < p_{m+1}.$$

Тада је $\pi(n - m - 1) = m$, па следи

$$n = \pi(n - m - 1) + (n - m - 1) + 1 \in B.$$

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са `https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf`

171

Пронаћи првих пет позитивних цијелих бројева за које је $n^2 - 1$ производ три различита проста броја

Доказ. Ако за позитиван број n, број $n^2 - 1$ је производ три различита проста броја, онда (у погледу $2^2 - 1 = 3$) имамо $n > 2$. Даље, када погледамо идентитет $n^2 - 1 = (n-1)(n+1)$, број n мора бити паран иначе остали фактори са десне стране би били парни, и $2^2 | n^2 - 1$. Штавише, бројеви $n - 1$ и $n + 1$ (који су оба > 1 јер је $n > 2$) не могу оба бити композитни јер у овом случају $n^2 - 1$ не може бити производ три различита проста броја различита проста броја. Тако да, један од бројева $n - 1$ и $n + 1$мора бити прост, а други мора бити производ два проста броја. За $n = 4$ имамо $n - 1 = 3, n + 1 = 5$ па услов није задовољен. Слично томе:
за $n = 6$ имамо $n - 1 = 5$, $n + 1 = 7$;

за $n = 8$ имамо $n - 1 = 7, n + 1 = 9 = 3^2$,
за $n = 10$ имамо $n - 1 = 9 = 3^2$, и
за $n = 12$ имамо $n - 1 = 11, n + 1 = 13$,
(ни један од ових бројева не задовољава постављени услов)
За $n = 14$ имамо $n - 1 = 13, n + 1 = 15 = 3 \cdot 5$. Тако да најмањи позитивни цијели број n за који је $n^2 - 1$ производ три различита проста броја је $n = 14$, за које је $n^2 - 1 = 3 \cdot 5 \cdot 13$. Пошто је $16^2 - 1 = 3 \cdot 5 \cdot 17$ видимо да је следећи број који задовољава услов $n = 16$. Сада, $18^2 - 1 = 17 \cdot 19, 20^2 - 1 = 19 \cdot 21 = 19 \cdot 3 \cdot 7$ и трећи број је $n = 20$, Следећи $22^2 - 1 = 7 \cdot 3 \cdot 23$ дакле четврти број је $n = 22$. Ако наставимо у овом правцу лако налазимо да је пети број $n = 32$ за који важи $32^2 - 1 = 3 \cdot 11 \cdot 31$. Пронађено је првих пет цијелих бројева n који задовољавају задати услов, и то су $14, 15, 20, 22$ и 32

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

172

Доказати да како су a, b, c три различита цијела броја, онда постоји бесконачно много позитивних цијелих бројева n таквих да су $a+n, b+n, c+n$ међусобно релативно прости

Доказ. Ако су цијели бројеви a, b, c различити, онда број

$$h = (a - b)(a - c)(a - c)$$

је различит од 0. У случају $h \neq \pm 1$, нека $q_1, ...q_2$ означава све просте бројеве > 3 који су дијелиоци h. Ако два или више бројева међу бројевима a, b, c су прости, биће $r = 1$ у супродном $r = 0$. Очигледно је је да ће најмање два броја $a+r, b+r, c+r$ бити непарна. Ако a, b, c дају три различита остатка при дијељењу са 3, поставимо онда r_0. Ово би значило да најмање два броја a, b, c не би била дијељива са 3.
Нека i означава један од бројева $1, 2, ..., s$. Знамо да постоји цијели број r_i такав да ни један од бројева $a + r_i, b + r_i, c + r_i$ није дијељив са q_i. По кинеској теореми о остацима, постоји бесконачно много цијелих бројева n таквих да

$$n \equiv r \pmod 2, n \equiv r_i \pmod 3,$$

и

$$\equiv r_i \pmod q)_i, i = 1, 2, ..., s$$

Требамо показати да бројеви $a + n, b + n$ и $c + n$ су међусобно релативно прости. предпоставмо да $(a + n, b + n) > 1$. Онда би постојао прост бројq такав да $q \mid a + n$ и $q \mid b + n$ пошто $q \mid a - b$, који имплицира да $q \mid h$ и $n \neq \pm 1$. Пошто је $n \not\equiv r \pmod 2$ и најмање два од бројева $a + r, b + r, c + r$ су непарни и не можемо имати да је $q = 2$. Слиједи, пошто је:

$$n = r_0 \pmod 3$$

и најмамње два броја од $a+r_0, b+r_0, c+r_0$ нису дијељива са 3 и најмамње два броја од $a+n, b+n, c+n$ нису дијељива са 3 не можемо имати $q=3$. Пошто је $q|h$ и узимајући у обзир дефиницију h, имамо $q=q_i$ и за одређено i из низа $1,2,...,s$. Међутим, с обзиром на:

$$n \equiv r_i \pmod{q)_i} \text{ или } n \equiv r_i \pmod{q}$$

и у погледу на чињеницу да ниједан од бројева:

$$a+r_i, b+r_i, c+r_i$$

није дијељив са q_i,
ниједан од бројева:

$$a+n, b+n, c+n$$

није дијељив са $q=q_i$
ослањајући се на $q \mid a+n$ и $q \mid b+n$. Тако да смо доказали $(a+n, b+n)=1$. Врло слично можемо показати да $(a+n, c+n)=1$ и $(b+n, c+n)=1$. Закључујемо да су бројеви $a+n$, $b+n$, и $c+n$ међусобно релативно прости. С обзиром на то да постоји бесконачно много таквих бројева n, доказ је потпун.

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

173

Доказати да сваки цијели број > 17 може бити представљен као збир три цијела броја > 1 који су узајамно релативно прости и показати како број 17 нема то својство

Доказ. Ако је n парно и > 8, онда је $n=6k$, $n=6k+2$, или $n=6k+4$, и у прва два случаја k је цијели број > 1. а у трећем случају k је позитиван цијели број. Формула

$$\begin{gathered} 6k = 2+3+(6(k-1)+1, \\ 6k+2 = 3+4+(6(k-1)+1 \\ 6k+4 = 2+3+(6k-1) \end{gathered}$$

показује да n је збир три релативно проста броја. Претпоставимо да n је непарно и > 17. Размотримо шест случајева: $n=12k+1$, $n=12k+3$, $n=12k+5$, $n=12k+7$, $12k+9$ и $n=12k+11$ гдје у прва три случаја k је цијели број > 1 и у последња три случаја k је позитиван цијели број. Имамо да је:
$12k-1=(6(k-1)-1)+(6(k-1)+5)+9$
гдје су бројеви $6(k-1)-1$, $6(6k-1)+5$, и 9, већи од 1 и релативно прости; заправо прва два броја нису дијељива са 3, и релативно су прости јер је $d \mid 6(k-1)-1$ и $d \mid 6(k-1)+5$ што подразумјева $d \mid 4$, гдје су бројеви које разматрамо непарни.

ако је $n = 12k + 3$, онда је $n = (6k - 1) + (6k + 1) + 3$;
ако је $n = 12k + 5$, онда је $n = (6k - 5) + (6k + 1) + 9$;
ако је $n = 12k + 7$, онда је $n = (6k + 5) + (6k - 1) + 3$;
ако је $n = 12k + 9$, онда је $n = (6k - 1) + (6k + 1) + 9$;

ако је $n = 12k + 11$, онда је $n = (6(k + 1) - 5) + (6(k + 1) + 1) + 3$ и лако провјеравамо да у сваком од наведених случајева имамо три услова > 1 и међусобно релативно прости. Број 17 нема тражено својство зато што у његовом случају $17 = a + b + c$ сва три броја a, b, c би били непарни. Ми међутим имамо да је $3 + 5 + 7 = 15 > 17$, и $3 + 5 + 11 > 17$, и у случају $3 < a < b < c$, имамо $a \geq 5, b \geq 7, c \geq 9$ а будући да је $a + b + c \geq 5 + 7 + 9 \geq 21 > 17$ закључујемо да 17 нема тражено својство

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

174

За било који природан број n постоји n узастопних сложених природних бројева. Доказати.

Доказ. Нека је $n \in N$. Следећи низ садржи н узастопних природних бројева, и сви чланови су му сложени бројеви:

$$\begin{gathered}(n+1)n(n-1)\cdot\ldots\cdot 3\cdot 2\cdot 1+2\\(n+1)n(n-1)\cdot\ldots\cdot 3\cdot 2\cdot 1+3\\\vdots\\(n+1)n(n-1)\cdot\ldots\cdot 3\cdot 2\cdot 1+n\\(n+1)n(n-1)\cdot\ldots\cdot 3\cdot 2\cdot 1+(n+1)\end{gathered}$$

конструкцијом оваквог низа узаступних природних бројева показано је да важи тврђење задатка. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

175

Доказати да су сви бројеви
(1) 10 001, 100 010 001, 1 000 100 010 001,...
(2) $n^4 + 4^n$, за свако $n \in N$
сложени.

Доказ. (1) Број $10001 = 73 \cdot 137$ је сложен.
За $k > 1, k$-ти елемент низа се може представити у облику

$$1 + 10^4 + \cdots + 10^{4k}$$

и важи:

$$1 + 10^4 + \cdots + 10^{4k} = \frac{10^{4k+4}-1}{10^4-1} = \frac{10^{2k+2}-1}{10^2-1} \cdot \frac{10^{2k+2}+1}{10^2+1} = \frac{(10^{2k}+\cdots+1)(10^{2k+2}+1)}{101}.$$

Број 101 је прост, па он дели бар један од бројева $10^{2k} + \cdots + 1$ и $10^{2k+2} + 1$, који су за $k > 1$ сигурно већи од 101, па је број

$$\frac{(10^{2k}+\cdots+1)(10^{2k+2}+1)}{101}$$

сложен.
(2) Разликујемо следеће случајеве:
1. Ако је н паран, тада је $n^4 + 4^n$ такође паран број већи од 2, па је сложен.
2. Ако је $n = 2k + 1$, за неки $k \in Z$, онда је

$$n^4 + 4^n = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot (2^k)^4,$$

што је сложен број. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

176

Наћи све природне бројеве који имају тачно 16 делилаца (укљу- чујући 1 и сам тај број) тако да је збир свих делилаца једнак 4 032.

Доказ. $4032 = 2^6 \cdot 3^2 \cdot 7$. Ако број има тачно 16 делилаца, онда он има једну од следећих факторизација: $p^{15}, p^7q, p^3q^3, p^3qr, pqrs$, где су p, q, r и s различити прости бројеви. Збир свих делилаца (који је једнак $4032 = 2^6 \cdot 3^2 \cdot 7$) у сваком од ових случајева је:

$$1 + p + p^2 \cdots + p^{15} = (1 + p)(1 + p^2)(1 + p^4)(1 + p^8);$$
$$(1 + p + p^2 \cdots + p^7)(1 + q) = (1 + p)(1 + p^2)(1 + p^4)(1 + q);$$
$$(1 + p + p^2 + p^3)(1 + q + q^2 + q^3) = (1 + p)(1 + p^2)(1 + q)(1 + q^2);$$
$$(1 + p + p^2 + p^3)(1 + q)(1 + r) = (1 + p)(1 + p^2)(1 + q)(1 + r);$$
$$(1 + p)(1 + q)(1 + r)(1 + s).$$

Фактор $1+p^2$ јавља се у прва четири случаја. Пошто број тог облика није дељив са 3, 4 или 7 ови случајеви не воде решењу. Не умањујући општост, можемо претпоставити да важи $p < q < r < s$. Запишимо у врсти редом просте бројеве:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots .$$

Тада број 4 032 треба написати као производ четири броја из низа:

$$3,\ 4,\ 6,\ 8,\ 12,\ 14,\ 18,\ 20,\ 24,\ 30,\ 32,\ 38,\ 42,\ \ldots .$$

1. Нека је $1+p=3$. Онда је $(1+q)(1+r)(1+s)=2^6\cdot 3\cdot 7$.
Ако је $1+q=4$, тада је $(1+r)(1+s)=2^4\cdot 3\cdot 7$. Како је

$$2^4\cdot 3\cdot 7=6\cdot 56=8\cdot 42=12\cdot 28=14\cdot 24$$

то постоје две могућности: $2\cdot 3\cdot 7\cdot 41=1722$ и $2\cdot 3\cdot 13\cdot 23=1794$. Ако је $1+q=6$, тада је $(1+r)(1+s)=2^5\cdot 7$. Како је

$$2^5\cdot 7=8\cdot 28=14\cdot 16,$$

то у овом случају нема решења.
Ако је $1+q=8$, тада је $(1+r)(1+s)=2^3\cdot 3\cdot 7$. Пошто је $2^3\cdot 3\cdot 7=12\cdot 14$ имамо решење $2\cdot 7\cdot 11\cdot 13=2002$. 2. Нека је $1+p=4$. Тада је $(1+q)(1+r)(1+s)=2^4\cdot 3^2\cdot 7$. Ако је $1+q=6$, тада је $(1+r)(1+s)=2^3\cdot 3\cdot 7$. Пошто је
$2^3\cdot 3\cdot 7=8\cdot 21=12\cdot 14$ добијамо решење $3\cdot 5\cdot 11\cdot 13=2145$.
Ако је $1+q\geq 8$, тада је $(1+q)(1+r)(1+s)\geq 8\cdot 12\cdot 14>2^4\cdot 3^2\cdot 7$, што значи да у том случају нема решења.
Даље, пошто је $6\cdot 8\cdot 12\cdot 14>2^6\cdot 3^2\cdot 7$, то нема других решења. Према томе, постоје четири природна броја која задовољавају услове задатка: 1 722, 1 794, 2 002 и 2 145. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

177

Доказати да има бесконачно много простих бројева облика $4k-1, k\in N$.

Доказ. Претпоставимо да таквих бројева има коначно много; нека су то $3,7,11,\ldots,p_n$. Посматрајмо број $P=4\cdot(3\cdot 7\ldots p_n)-1$. Број P већи је од свих наведених простих бројева и има облик $4k-1$;дакле, сложен је. Пошто је

$$P+1=4\cdot(3\cdot 7\ldots p_n)$$

и $(P,P+1)=1$, то је P узајамно прост са свим простим бројевима $3,7,11,\ldots,p_n$, а како је P и непаран број, сви његови прости фактори су облика $4k+1$. Но, то је немогуће јер производ два броја облика $4k+1$ има облик

$$(4k_1+1)(4k_2+1)=4\cdot(4k_1k_2+k_1+k_2)+1,$$

а P је облика $4k-1$. Контрадикција.

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Ико диновић, 2004.

178

Дато је 15 природних бројева $1 < n_1, n_2, \ldots, n_{15} \leq 2003$. Ако је за све $i, j \in \{1, 2, \ldots, 15\}, i \neq j, (n_i, n_j) = 1$, доказати да је бар један од датих бројева прост.

Доказ. Нека је p_i најмањи прост број који дели n_i. Тврђење задатка следи из чињенице да су $p_1, p_2, \ldots, p_{15}$ међусобно различити прости бројеви и да је 15-ти прост број (у низу простих бројева) 47 ($47^2 = 2209 > 2003$). □

(**Данијела Матановић 38/18 Д**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

179

Пронаћи пет најмањих позитивних бројева n таквих да сваки од бројева $n, n+1, n+2$ је производ два различита проста броја. Доказати да не постоји 4 узастопна цијела броја са овим својством. Показати на примјеру да постоји 4 позитивна броја таква да сваки од њих има два проста дијелиоца

Доказ. $n = 33 (n = 3 \cdot 11, n + 1 = 2 \cdot 17, n + 2 = 5 \cdot 7$
$n = 85 (n = 5 \cdot 17, n + 1 = 2 \cdot 43, n + 2 = 3 \cdot 29$
$n = 93 (n = 3 \cdot 31, n + 1 = 2 \cdot 47, n + 2 = 5 \cdot 19$
$n = 141 (n = 3 \cdot 47 \cdot 11, n + 1 = 2 \cdot 71, n + 2 = 11 \cdot 13$
$n = 201 (n = 3 \cdot 67, n + 1 = 2 \cdot 101, n + 2 = 7 \cdot 29$

Не постоји четири узастопна позитивна цијела броја таква да сваки од њих је производ два разлилчита проста броја зато што сваки од та четири броја мора бити дијељив са 4. Примјер четири узастопна броја таква да сваки од њих имају тачно два проста дијелиоца су бројеви $33 = 3 \cdot 11, 34 = 2 \cdot 17, 35 = 5 \cdot 7, 36 = 2^2 \cdot 3^2$.
Напомена: Не можемо доказати да постоји бесконачно много бројаева n таквих да сваки од бројева $n, n + 1$ и $n + 2$ је производ два проста броја.

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

180

За који прост број p је и број $8p^2 + 1$ такође прост?

Доказ. Ако је $p = 2$ тада је $8 \cdot 2^2 + 1 = 33$ а ово је сложен број.Ако је $p = 3$ онда је $8 \cdot 3^2 + 1 = 73$ прост број.Нека је, сада p прост број већи од 3.Он ће тада бити облика

$p = 3k + 1$ ili $p = 3k - 1$. Сада је:
$8(3k \pm 1)^2 + 1 = 72k^2 \pm 48k + 9$
а овај број је сложен јер је дељив са 3. Па закључујемо да је $8p^2 + 1$ прост број, једино када је $p = 3$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

181

Ako je p prost broj dokazati da je $p^{2011} + p^{2013}$ složen.

Доказ. Ako je $p = 2$ tada je $2^{2011} + 2^{2013}$ zbir dva parna broja,koji je paran broj, pa time i složen.Neka je broj prost broj $p \leq 3$, on je onda i neparan.Ali, i neparan stepen neparnog broja će biti neparan, pa je zbir $p^{2011} + p^{2013}$ zbir dva neparna broja, a to je paran broj.Pa pošto je paran on je i složen, što je i trebalo pokazati. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

182

Наћи p ако су:
a)$p, 2p + 1, 4p + 1$ прости бројеви.
b)p и $8p^2 + 1$ прости бројеви.

Доказ. *a*) Ако је $p = 2$, имамо $2p + 1 = 5$ и $4p + 1 = 9$, па с обзиром да 9 није прост, $p = 2$ не задовољава услов задатка. За $p = 3$, имамо $2p + 1 = 7$ и $4p + 1 = 13$, тако да $p = 3$ јесте решење. За прост број $p > 3$,према претходном задатку знамо да постоје две могућности: или је $p = 6k + 1$ или $p = 6k - 1$. У првом случају $2p + 1 = 12k + 3 = 3m$, а у другом $4p + 1 = 24k - 3 = 3n$. То значи да је за сваки прост број $p > 3$ увек један од бројева $2p + 1, 4p + 1$ дељив са 3, па самим тим није прост и ниједно такво p не задовољава услов задатка. Број је једино решење.

b) Ако је $p = 2$, имамо $8p^2 + 1 = 33$, па 2 није решење. Уколико је $p = 3$, $8p^2 + 1 = 73$, па 3 јесте решење. Даље, ниједан прост број $p > 3$ није решење зато што важи $8p^2 + 1 \equiv -(p^2 - 1) \equiv -(p - 1)(p + 1) \equiv 0 \pmod 3$. То следи из чињенице да је тачно један од три узастопна броја $p - 1, p, p = 1$ дељив са 3, при чему то сигурно није p зато што је прост и већи од 3 Закључујемо да је поново број 3 једино решење. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

183

Показати да $f(n) = n^5 + n^4 + 1$ није прост, за $n > 1$.

Доказ. Показаћемо да се полином $f(n)$ може представити као производ фактора нижег степена који такође имају целобројне коефицијенте. С обзиром да је слободан члан једнак 1, уколико би постојао линеарни фактор, он би морао да буде или облика $n+1$ или $n-1$. Како је $f(1) \neq 0$ и $f(-1) \neq 0$, закључујемо да нема линеарног фактора.
Тражимо квадратне и кубне факторе. Постоје две могућности:

$$(1) n^5 + n^4 + 1 = (n^2 + an + 1)(n^3 + bn^2 + cn + 1)$$
$$(2) n^5 + n^4 + 1 = (n^2 + an - 1)(n^3 + bn^2 + cn - 1)$$

Решимо први случај. Кад измножимо и распишемо десну страну, добијамо

$$n^5 + n^4 + 1 = n^5 + (a+b)n^4 + (ab + c + 1)n^3 + (ac + b + 1)n^2 + (a + c)n + 1.$$

Упоређујући коефицијенте на левој и десној страни, добијамо систем од четири једначине по a, b, c:

$$a + b = 1, ab + c + 1 = 0, ac + b + 1 = 0, a + c = 0$$

чија су решења

$$b = 0, a = 1, c = -1.$$

Стога,

$$n^5 + n^4 + 1 = (n^2 + n + 1)(n^3 - n + 1)$$

Други случај ни нема потребе разматрати зато што смо управо нашли једну факторизацију полинома f(n), што значи да није прост. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

184

Ако су $2n + 1$ и $3n + 1$ потпуни квадрати, $n \in \mathbb{N}$, dokazati da onda $5n + 3$ није прост број.

Доказ. Нека је $2n + 1 = a^2$, $3n + 1 = b^2$ за неке $a, b \in \mathbb{N}$. Тада $5n + 3 = 4(2n + 1) - (3n + 1) = 4a^2 - b^2 = (2a + b)(2a - b)$. Претпоставимо да је $2a - b = 1$. Тада се претходна једнакост своди на $5n + 3 = 2a + b$. Затим, $2b = 2a + b - (2a - b) = 5n + 3 - 1 = 5n + 2$. И коначно, $(b - 1)^2 = b^2 - 2b + 1 = (3n + 1) - (5n + 2) + 1 = -2n$. Добија се $(b - 1)^2 = -2n < 0$, што је контрадикција, па мора бити $2a - b \neq 1$. Из једнакости $5n + 3 = (2a + b)(2a - b)$ видимо да је $2a - b$ природан број већи од 1, зато што су $5n + 3$, $2a + b \in \mathbb{N}$. Према томе, није прост број јер је дељив са $2a - b$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

185

За природне бројеве a,b,c,d важи $a^2+b^2=c^2+d^2$. Да ли је $a+b+c+d$ сложен број?

Доказ. $(a+b+c+d)^2=a^2+b^2+c^2+d^2+2ab+2ac+2ad+2bc+2bd+2cd=2(a^2+b^2+ab+ac+ad+bc+bd+cd)$
Значи,$(a+b+c+d)^2$ је паран број, па је и $a+b+c+d$ паран, дакле сложен. □

(**Јована Шубарић 11/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

186

Збир два природна броја једнак је 30030. Доказати да њихов производ није дјељив са 30030.

Доказ. Претпоставићемо да је производ природних бројева x и $30030-x$ гдје је $(x<30030)$ дјељив са 30030,
тј. да је $x(30030-x)=30030k$.
Тада је $x^2=30030(x-k)$,
тј. број x^2 је дјељив са 30030. Тада је x дјељиво сваким простим фактором броја 30030 .
Како је $30030=2\cdot3\cdot5\cdot7\cdot11\cdot13$,
то је x дјељиво са 30030, па је $x\geq30030$, што је контрадикција. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

187

Доказати да степен простог броја не може бити савршен број.

Доказ. Прво ћемо се подсјетити шта је то савршен број .
Савршен број је природан број који је једнак збиру својих позитивних дјелилаца, укључујући и број 1, али не рачунајући сам тај број.
Када смо обновили градиво можемо наставити са рјешавањем овог задатка.
Претпоставимо супротно. Нека је p прост број, такав да је број p^α савршен . Тада је $\sigma(p^\alpha)=2p^\alpha$, па је

$$2p^\alpha=\frac{p^{\alpha+1}-1}{p-1}$$

тј.

$$2p^{\alpha} = p^{\alpha+1} + 1$$

Одакле слиједи да је $2 > p$. Дакле, контрадикција. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

188

Наћи све природне бројеве $n < 1979$ који задовољавају следећи услов: ако је m природан број, $1 < m < n$ и $(m, n) = 1$, онда је m прост број.

Доказ. Нека је S скуп свих природних бројева за које важе наведени услови. Ако је $n \in S$ и $p^2 < n$, где је p прост број, онда n и p^2 нису узајамно прости бројеви јер p^2 није прост број. Према томе $p \mid n$. Ако је $n > 49$ и $n \in S$ онда је сваки од бројева 2, 3, 5, 7 дјелилац броја n. Зато је $n \geq 2 \cdot 3 \cdot 5 \cdot 7 = 210 > 11^2$ па и $11 \mid n$.Даље слиједи $n \geq 210 \cdot 11 = 2310 > 1979$, што је контрадикција. Зато је $S \subset \{1, 2, \ldots, 49\}$.
Нека је $n > 25$. Тада $n \in S$ ако и само ако је број n дјељив са $2 \cdot 3 \cdot 5 = 30$. Такав број је само 30.
Нека је $9 < n \leq 25$. Тада $n \in S$ ако и само ако је број n дјељив са $2 \cdot 3 = 6$. То важи за бројеве 12, 18, 24.
Нека је $4 < n \leq 9$. Тада $n \in S$ ако и само ако је n паран број. Дакле, $6 \in S$, $8 \in S$. Лако се провјерава да сваки од бројева 2, 3, 4 припада скупу C. Према томе, $S = \{2, 3, 4, 6, 8, 12, 18, 24, 30\}$ □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

189

Доказати да је природан број $n > 1$ прост ако и само ако важи

$$[\tfrac{n}{1}] + [\tfrac{n}{2}] + \cdots + [\tfrac{n}{n}] = 2 + [\tfrac{n-1}{1}] + [\tfrac{n-1}{2}] + \cdots + [\tfrac{n-1}{n-1}]$$

Доказ. Како је $[\frac{n}{1}] = n, [\frac{n}{n}] = 1 = 1$ и $[\frac{n-1}{1}] = n - 1$ то из дате једнакости слиједи

$$[\tfrac{n}{2}] + \cdots + [\tfrac{n}{n-1}] = [\tfrac{n-1}{2}] + \cdots + [\tfrac{n-1}{n-1}].$$

С обзиром на то да за свако $k \in \{2, 3, \ldots, n-1\}$ важи $[\frac{n}{k}] \geq [\frac{n-1}{k}]$, то због претходне једнакости за све k важи $k \in \{2, 3, \ldots, n-1\}$ важи $[\frac{n}{k}] = [\frac{n-1}{k}]$. Ако би n био сложен број, онда би за неко $k \in \{2, 3, \ldots, n-1\}$ број $\frac{n}{k}$ био цио, па би важило

$$\tfrac{n}{k} = [\tfrac{n}{k}] = [\tfrac{n-1}{k}] \leq \tfrac{n-1}{k}$$

Дакле, n мора бити прост број. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

190

Нека је p_n n-ти прост број. Доказати да за сваки природан број $n > 4$ важи неједнакост $p_n > 2n$.

Доказ. За $n = 5$ тврђење важи јер је $p_5 = 11 > 10$. Ако је $p_n > 2n$, онда је $p_{n+1} \geq p_n + 2 > 2n + 2 = 2(n + 1)$.
Дакле, за свако $n > 4$ је $p_n > 2n$. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

191

Доказати једнакост

$$\tau(1) + \tau(2) + \cdots + \tau(n) = [\tfrac{n}{1}] + [\tfrac{n}{2}] + \cdots + [\tfrac{n}{n}].$$

Доказ. Приметимо најпре да је

$[\frac{n+1}{k}] =$
1. $[\frac{n}{k}]$, $k \nmid n + 1$
2. $[\frac{n}{k}] + 1$, $k \mid n + 1$.

Заиста, ако је $n + 1 = qk + r$ и $1 \leq r \leq k - 1$, тада је

$$n = qk + r - 1 \text{ и } [\tfrac{n+1}{k}] = [\tfrac{n}{k}] = q.$$

Ако је $n + 1 = qk$ онда је $[\frac{n+1}{k} = q]$ и $[\frac{n}{k}] = q - 1$.
Дакле, имамо да је
$[\frac{n+1}{1}] + [\frac{n+1}{2}] + \cdots + [\frac{n+1}{n+1}] = [\frac{n}{1}] + [\frac{n}{2}] + \cdots + [\frac{n}{n}] + \tau(n + 1)$.
Ако је

$$[\tfrac{n}{1}] + [\tfrac{n}{2}] + \cdots + [\tfrac{n}{n}] = \tau(1) + \tau(2) + \cdots + \tau(n),$$

онда је
$[\frac{n+1}{1}] + [\frac{n+1}{2}] + \cdots + [\frac{n+1}{n+1}] = \tau(1) + \tau(2) + \cdots + \tau(n) + \tau(n + 1)$,
па тврђење важи на основу принципа математичке индукције, јер тврђење очигледно важи за $n = 1$. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

192

Доказати да за природне бројеве a, b, c важи:

$$abc = [a, b, c] \cdot (ab, bc, ca)$$

Доказ. Нека је :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$$

Неки од бројева $\alpha_i, \beta_i, \gamma_i$ могу бити једнаки нули тада би имали следећи израз :

$$[a, b, c] = p_1^{\max(\alpha_1, \beta_1, \gamma_1)} \dots p_k^{\max(\alpha_k, \beta_k, \gamma_k)}$$

$$(ab, bc, ca) = p_1^{\min(\alpha_1+\beta_1, \beta_1+\gamma_1, \gamma_1+\alpha_1)} \dots p_k^{\min(\alpha_k+\beta_k, \beta_k+\gamma_k, \gamma_k+\alpha_k)}$$

Пошто је

$$\max(\alpha_i, \beta_i, \gamma_i) + \min(\alpha_i + \beta_i, \beta_i + \gamma_i, \gamma_i + \alpha_i) = \alpha_i + \beta_i + \gamma_i$$

За $(i = \overline{1, k})$
Ако је γ_i највећи , најмањи збир је онда $\alpha_i + \beta_i$.
Одакле слиједи да је тврдња тачна. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

193

Да ли постоји природан број n такав да се $n!$ завршава са 11 нула ?

Доказ. За рјешавање овог задатка користићемо једну олакшицу , како можемо знати колико један факториал број има нула ? Врло једноставно , на примјер број 50!

$$\left[\frac{50}{5}\right] + \left[\frac{50}{25}\right] + \left[\frac{50}{125}\right] = 10 + 2 + 0 = 12$$

Из овог примјера видимо да број 50! има 12 нула. Сада ћемо пробати број 49 јер број 50 није .

$$\left[\frac{49}{5}\right] + \left[\frac{49}{25}\right] + \left[\frac{49}{125}\right] = 9 + 1 + 0 = 10$$

Број 49! има 10 нула . Из овог закључујемо да не постоји број n такав да се $n!$ завршава са 11 нула. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

194

Колико највише дјелилаца може да има природан број мањи од 1994?

Доказ. Број дјелилаца природног броја чија је канонска факторизација $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ је :

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$$

Како је $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 > 1994$, то у канонској факторизацији природног броја који није већи од 1994 могу да учествују највише четири проста броја .
Довољно је одредити број дјелилаца следећих бројева :

$$2^{10}, 2^9 \cdot 3, 2^8 \cdot 3, 2^7 \cdot 3^2, 2^7 \cdot 3 \cdot 5$$

$$2^6 \cdot 3^3, 2^6 \cdot 3 \cdot 5, 2^5 \cdot 3^3, 2^5 \cdot 3^2 \cdot 5, 2^4 \cdot 3^4$$

$$2^4 \cdot 3^3 \cdot 5, 2^4 \cdot 3 \cdot 5 \cdot 7, 2^2 \cdot 3^2 \cdot 5 \cdot 7$$

Највећи број дјелилаца међу њима има број $2^4 \cdot 3 \cdot 5 \cdot 7 = 1680$ и тај број дјелилаца једнак је $5 \cdot 2 \cdot 2 \cdot 2 = 40$ □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

195

Природан број $n > 1$ је сложен ако и само ако има прост фактор p, такав да је $p \leq \sqrt{n}$.

Доказ. Ако n има прост фактор $p \leq \sqrt{n}$, онда је он очигледно сложен број. Обрнуто, ако је p најмањи прост фактор сложеног броја n, тада постоји природан број q такав да је $n = pg$, и при том је $q \geq p$. Одатле следи да је $p \leq \sqrt{n}$. □

(**Никола Цупара 08/17 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

196

Одредити најмањи природан број чија је половина потпун квадрат, трећина потпун куб и петина потпун пети степен.

Доказ. Тражени број n мора бити дељив са 2, 3 и 5 и, због минималности, нема других простих фактора. Нека је $n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$. Из услова задатка следи да је:

$$\frac{n}{2} = 2^{\alpha-1} \cdot 3^\beta \cdot 5^\gamma = a^2,$$
$$\frac{n}{3} = 2^\alpha \cdot 3^{\beta-1} \cdot 5^\gamma = b^3,$$
$$\frac{n}{5} = 2^\alpha \cdot 3^\beta \cdot 5^{\gamma-1} = c^5,$$

где су a, b и c природни бројеви. Тада је α најмањи непаран природан број дељив са 3 и 5, β најмањи природан број дељив са 2 и 5 који при дељењу са 3 даје остатак 1 и γ најмањи природан број дељив са 2 и 3 који при дељењу са 5 даје остатак 1.
Према томе, $\alpha = 15$, $\beta = 10$ и $\gamma = 6$. Тада је $n = 2^{15} \cdot 3^{10} \cdot 5^6 = 30\ 233\ 088\ 000\ 000$. □

(**Никола Цупара 08/17 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

197

Из скупа $\{1, 2, \cdots, 2n\}$ на произвољан начин изабран је $n+1$ број. Доказати да међу изабраним бројевима увек постоји број дељив неким другим од изабраних бројева.

Доказ. Нека су $a_1, a_2, \cdots, a_{n+1}$ произвољни бројеви из скупа $\{1, 2, \cdots, 2n\}$. Сваки од њих се може записати у облику $a_i = 2^{k_i} b_i$, где је b_i непаран. Тада су $b_1, b_2, \cdots, b_{n+1}$ непарни бројеви из интервала $[1, 2n-1]$, а како у том интервалу постоји само n непарних бројева, два су једнака, тј. за неке $i, j \in \{1, \cdots, n-1\}$, $i \neq j$ је $b_i = b_j$, па један од бројева a_i, a_j дели други. □

(**Никола Цупара 08/17 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

198

Нека је p_n n-ти прост број. Доказати да за сваки природан број $n > 4$ важи неједнакост $p_n > 2n$.

Доказ. За $n = 5$ тврђење важи јер је $p_5 = 11 > 10$. Ако је $p_n > 2n$, онда је $p_{n+1} \geq p_n + 2 > 2n + 2 = 2(n+1)$. Дакле, за свако $n > 4$ је $p_n > 2n$. □

(**Никола Цупара 08/17 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

199

Одредити најмањи природан број који је тачно 100 пута већи од броја својих делилаца, укључујући 1 и сам тај број.

Доказ. Према услову задатка имамо да је

$$n = 2^{\alpha_1} 5^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k} = 2^2 5^2 (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = 100\tau(n).$$

(1) Ако су 2 и 5 једини прости делиоци броја n имамо да је

$$2^{\alpha_1} 5^{\alpha_2} = 2^2 5^2 (\alpha_1 + 1)(\alpha_2 + 1),$$

па је очигледно $\alpha_1 \geq 2$ и $\alpha_2 \geq 2$. Ниједан од ових бројева не може бити 2, јер би тада десна страна била дељива са 3, а лева не. Дакле, $\alpha_1 \geq 3$ и $\alpha_2 \geq 3$. За $\alpha_2 = 3$ имамо решење $\alpha_1 = 4$, тј. $n = 2000$, што је очигледно најмање решење у овом случају.

(2) Нека сада n има и простих делилаца различитих од 2 и 5. Треба утврдити може ли бити $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) < 20$. Ако је $\alpha_1 > 2$ или $\alpha_2 > 2$, неједнакост не може бити испуњена јер је број с леве стране тада бар $4! = 24$. Значи, остаје могућност $\alpha_1 = \alpha_2 = 2$

и $\alpha_3 = 1$, па добијамо да је $2^2 5^2 p_3 = 100 \cdot 3 \cdot 3 \cdot 2$, што је немогуће јер је десна страна дељива са 9, а лева није.
Значи тражени број је 2000. □

(**Никола Цупара 08/17 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

200

Доказати да је сваки прост број $p > 3$ облика $6k + 1$ или $6k + 5$.

Доказ. Сви ненегативни цијели бројеви су облика:
$6k$, $6k + 1$, $6k + 2$, $6k + 3$, $6k + 4$ и $6k + 5$.
Бројеви облика $6k$, $6k + 2$ и $6k + 4$ су парни бројеви, па самим тим не могу бити прости.
Бројеви облика $6k + 3$ су дјељиви бројем 3, јер је $6k + 3 = 3 \cdot (2k + 1)$, што је очито дјељиво са 3.
Остају нам само бројеви облика $6k + 1$ и $6k + 5$, што значи да су сви прости бројеви већи од 3 или облика $6 + 1$ или облика $6 + 5$. Овим је наше тврђење доказано.
□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет из књиге Теорија бројева:
`https://www.vladimirbozovic.net/univerzitet/bozovic/wp-content/uploads/2010/01/Zbirka-rijesen pdf`

201

Сваки број облика $3n - 1$ је дјељив неким простим бројем облика $3k - 1$. Доказати.

Доказ. Сви ненегативни цијели бројеви су облика:
$3k$, $3k + 1$ и $3k + 2$.
Бројеви облика $3k$ су дјељиви бројем 3, ра осим броја 3, нема других простих бројева овог облика. Бројеви облика $3k + 2$ се другачије могу записати као $3k - 1$. Из овога закључујемо да су сви прости бројеви облика $3k + 1$ или $3k - 1$.
Претпоставимо да број $3n - 1$ нема простих чинилаца облика $3k - 1$. То значи да су сви његови чиниоци облика $3k + 1$. Узмимо за примјер да се ради о броју који има само два чиниоца. Тада је прозвод његових чинилаца облика $(3k + 1)(3j + 1)$. То се може средити на начин што помножимо сваки члан са сваким:

$$(3k + 1)(3j + 1) = 3kj + 3k + 3j + 1$$

Затим извучемо заједничку 3 тамо гдје је то могуће:

$$3kj + 3k + 3j + 1 = 3(kj + k + j) + 1$$

Нека је $kj + k + j = n$, тада је:

$$3(kj + k + j) + 1 = 3n + 1$$

Како се ради о броју који се састоји од само два чиниоца, када их помножимо, добијамо да је то број облика $3n+1$. Међутим наш почетни број је био $3-1$. Као што видимо:

$$3n+1 \neq 3n-1$$

То значи да смо добили другачији број од почетног, што није могуће. Из овога слиједи да наш број $3n-1$ мора имати чинилац облика $3k-1$, што значи да су сви бројеви облика $3n-1$ дјељиви неким простим бројем облика $3k-1$, чиме је доказано наше тврђење.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет из књиге Теорија бројева: `https://www.vladimirbozovic.net/univerzitet/bozovic/wp-content/uploads/2010/01/Zbirka-rijesen pdf`

202

Ако је p прост број већи од 3, доказати да је p^2-1 дељив са 24.

Доказ. С обзиром да је p прост број, n је и непаран, па је

$$p^2-1=(p+1)\cdot(p-1)$$

Производ два парна броја, који су и узастопни парни бројеви. Па је један од њих дјељив са 2 а други са 4, зато је њихов производ $(p+1)\cdot(p-1)$ дјељив са 8. Такође, пошто је p прост број он сигурно није дјељив са 3, а $p-1$ и $p+1$ су му претходник и следбеник, од којих је један сигурно дјељив са 3. Па како смо показали да је овај производ дјељив са 8 и са 3, то је он дјељив и са 24.

□

(**Јакша Мрдак 23/17 Д**)

203

За који прост број p је и број $8p^2+1$ такође прост?

Доказ. Ако је

$$p=2$$

тада је

$$8\cdot 2^2+1=33$$

,

а ово је сложен број.

Ако је

$$p=3$$

онда је

$$8 \cdot 3^2 + 1 = 73$$

,

прост број.

Нека је сада, p прост број већи од 3. Он ће тада бити облика $p = 3k + 1$ или $p = 3k - 1$.

Сада је:

$8(3k \pm 1)^2 + 1 = 72k^2 \pm 48k + 9$

А овај број је сложен јер је дјељив са 3. Па закључујемо да је $8p^2 + 1$ прост број, једино када је $p = 3$.

□

(Јакша Мрдак 23/17 Д)

204

Да ли је $3^n + 3^{n+1} + 3^{n+2}$ прост или сложен ?

Доказ. Због могућности да се израз $3^n + 3^{n+1} + 3^{n+2}$ запише као производ

$3^n + 3^{n+1} + 3^{n+2} = 3^n \cdot (1 + 3 + 3^2) = 3^n \cdot 13$

Једноставно закључујемо да је то сложен број.

□

(Јакша Мрдак 23/17 Д)

205

Одредити све просте бројеве p за које је и број $3^p + p^3$ прост.

Доказ. За $p = 2$ је и $32 + 23 = 17$ прост, а за друге просте бројеве p, који су уз то и непарни, збир $3^p + p^3$ је збир два непарна броја, па је он паран, а тиме и сложен. Дакле, број $3^p + p^3$ је прост једино за $p = 2$.

□

(Јакша Мрдак 23/17 Д)

206

Постоји ли прост број п тако да и бројеви $3p + 1$ и $5p + 1$ буду прости?

Доказ. Постоји, То је број $p = 2$, јер су тада $3 \cdot 2 + 1 = 7$ и $5 \cdot 2 + 1 = 11$ прости бројеви. Више од овог не би било могуће јер би за било који други прост број $p \geq 3$, због његове непарности, бројеви $3p + 1$ и $5p + 1$ били парни па тиме и сложени.

□

(Јакша Мрдак 23/17 Д)

207

Наћи све парове простих бројева p и q, такве да је:

$$p^3 - q^5 = (p+q)^2$$

Доказ. Претпоставимо прво да ниједан од бројеа p и q није прост. Тада ниједан од њих није дјељив са 3, па је $p^2 \equiv_3 q^2 \equiv_3 1$.

Из једнакости дате у задатку имамо да је и $p - q \equiv_3 (p+q)^2$. Уколико и p и q дају остатак 1 или 2 по модулу 3, лијева страна конгруенције је 0, док десна није, што је немогуће.

Такође, уколико p и q дају различите остатке при дијељењу са 3, тада је десна страна конгруенције једнака 0, а лијева није, што такође није могуће.

Значи да један од бројева p и q мора бити једнак 3.

а) За $p = 3$:

Тада је $27 - q^5 > 0$, што је очигледно немогуће.

б) За $q = 3$:

Тада је $p^3 - 243 = (p+3)^2$, па је онда и $p^3 - p^2 - 6p = p(p^2 - p - 6) = 252 = 2^2 \cdot 3^3 \cdot 7$.

Тиме закључујемо да је p један од бројева $2, 3, 7$.

Како је $4 - 2 - 6 < 0$ и $9 - 3 - 6 = 0$, а $7(49 - 7 - 6) = 7 \cdot 36 = 252$, то је једино могуће за $q = 7$.

Добијамо да је једино рјешење овог задатка пар $(3, 7)$. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

208

Доказати да за свако $n \in N$, број $2^{2^n} + 2^{2^{n-1}} + 1$ има најмање n различитих простих дјелилаца.

Доказ. Тврдђење доказујемо индукцијом по n.

За $n = 1$ је $2^{n^1} + 2^{2^0} + 1 = 7$.

За сваки реалан број x важи једнакост:

$$x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$$

па је и:

$$2^{2^{n+1}} + 2^{2^n} + 1 = (2^{2^n} - 2^{2^{n-1}} + 1)(2^{2^n} + 2^{2^{n-1}} + 1)$$

Имамо и да је $(2^{2^n} - 2^{2^{n-1}} + 1, 2^{2^n} + 2^{2^{n-1}} + 1) = 1$, јер ако би ови бројеви имали заједнички прост фактор $p > 2$ ($p \neq 2$ јер су бројеви непарни), онда би било:

$$p \mid (2^{2^n} - 2^{2^{n-1}} + 1) - (2^{2^n} + 2^{2^{n-1}} + 1) = 2 \cdot 2^{2^{n-1}}$$

што је немогуће јер је p непаран прост број.

Дакле, по претпоставци, ако $2^{2^n} + 2^{2^{n-1}} + 1$ има најмање n различитих простих дјелилаца, онда $2^{2^{n+1}} + 2^{2^n} + 1$ има најмање $n+1$ различитих простих дјелилаца. Овим је доказ завршен. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

209

За природне бројеве m и n кажемо да су пријатељски бројеви ако је сваки од њих једнак збиру правих дјелилаца другог. Доказати следеће тврђење: Ако су $p = 3 \cdot 2^{k-1} - 1, q = 3 \cdot 2^k - 1$ и $r = 9 \cdot 2^{2k-1} - 1$ прости бројеви, онда су $A = 2^k pq$ и $B = 2^k r$ пријатељски бројеви.

Доказ. Збир свих позитивних дјелилаца броја $n = \prod_{i=1}^{k} p_i^{a_i}$ је:

$$\sigma(n) = \prod_{i=1}^{k} \sum_{j=0}^{a_1} p_i^j$$

Тако збир дјелилаца броја A износи:

$$\sigma(A) = (1 + 2 + \cdots + 2^k)(1 + p)(1 + p) = (2^{k+1} - 1) \cdot 9 \cdot 2^{2k-1}$$

Збир свих дјелилаца броја B је исти:

$$\sigma(B) = (1 + 2 + \cdots + 2^k)(1 + r) = (2^{k+1} - 1) \cdot 9 \cdot 2^{2k-1}$$

Такође је:

$$A + B = 2^k(pq + r) = 2^k((3 \cdot 2^{k-1} - 1)(3 \cdot 2^k - 1) + 9 \cdot 2^{2k-1} - 1) = 2^k(9 \cdot 2^{2k} - 9 \cdot 2^{k-1}) =$$

$$= 2^{2k-1} \cdot 9(2^{k+1} - 1)$$

Збир правих дјелилаца броја A је $\sigma(A) - A = (A + B) - A = B$, а збир правих дјелилаца броја B је $\sigma(B) - B = (A + B) - B = A$.

Тиме је доказано да су A и B пријатељски бројеви. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

210

Нека су p и q прости бројеви за које важи $q \mid p - 1$ и $p \mid q^3 - 1$. Доказати да је тада $p = q^2 + q + 1$.

Доказ. Важи да $p \mid q^3 - 1 = (q - 1)(q^2 + q + 1)$. С обзиром да је p прост, значи да $p \mid q - 1$ или $p \mid q^2 + q + 1$.

Из услова задатка $q \mid p - 1$ слиједи да је $q \leq p - 1$ па је онда и $p \geq q + 1 > q - 1$ те онда $p \mid q$ не може бити тачно.

Мора бити $p \mid q^2 + q + 1$.

Користећи тако добијену релацију $p \mid q^2 + q + 1$ и $q \mid p - 1$ добија се да важи $pq \mid (p - 1)(q^2 + q + 1)$ тј. $pq \mid pq^2 + pq + p - q^2 - q - 1$, а одатле даље слиједи $pq \mid q^2 + q + 1 - p$.

То значи да је или $q^2 + q + 1 - p = 0$ или $q^2 + q + 1 - p \geq pq$.

Ако би важила друга неједнакост, онда би важило и $q^2 + q + 1 \geq p(q + 1)$, а како је $p \geq q + 1$ онда би било и да је $q^2 + q + 1 \geq (q + 1)^2 = q^2 + 2q + 1$, а то представља контрадикцију.

Стога закључујемо да је $q^2 + q + 1 = p$, те је доказ тако завршен. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

211

Доказати да ако је n природан број већи од 1, онда $n^4 + 4^n$ није није прост.

Доказ. Ако је n парно, онда је и $n^4 + 4^n$ парно и веће од 2, па то није прост број.

Значи треба још показати да је тачна тврдња уколико је n непарно.

За $n = 2k + 1$, користећи Сопхие Германн идентитет:

$$a^4 + 4b^4 = a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - (2ab)^2 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$$

правимо следећу трансформацију:

$$n^4 + 4^n = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot (2^k)^4$$

$$n + 4^n = (n^2 + 2 \cdot 2^{2k} + 2n \cdot 2^k)(a^2 + 2 \cdot 2^{2k} - 2n \cdot 2^k)$$

Одавде видимо да $n^4 + 4^n$ није прост. Овим је доказ завршен. □

212

Доказати да за сваки прост број p важи: $(p-2)! \equiv 1 \pmod{p}$

Доказ. Према Вилсоновој теореми важи :

$$\begin{gathered}(p-1)! + 1 \equiv 0 \pmod{p} \\ (p-2)! \cdot (p-1) + 1 \equiv 0 \pmod{p} \\ (p-2)! \cdot p - (p-2)! + 1 \equiv 0 \pmod{p} \\ p(p-2)! - ((p-2)! - 1) \equiv 0 \pmod{p} \\ (p-2)! - 1 \equiv 0 \pmod{p}\end{gathered}$$

Одакле следи:

$$(p-2)! \equiv 1 \pmod{p}$$

□

(**Николина Јеловац 13/18 Д**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

213

Доказати да за сваки прост број p важи: $(p-2)! \equiv 1 \pmod{p}$

Доказ. Према Вилсоновој теореми важи :

$$\begin{gathered}(p-1)! + 1 \equiv 0 \pmod{p} \\ (p-2)! \cdot (p-1) + 1 \equiv 0 \pmod{p} \\ (p-2)! \cdot p - (p-2)! + 1 \equiv 0 \pmod{p} \\ p(p-2)! - ((p-2)! - 1) \equiv 0 \pmod{p} \\ (p-2)! - 1 \equiv 0 \pmod{p}\end{gathered}$$

Одакле следи:

$$(p-2)! \equiv 1 \pmod{p}$$

□

(**Николина Јеловац 13/18 Д**) задатак преузет са
http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1

214

Одредити све просте бројеве p за које су и бројеви $p+3$, p^2+3, p^3+3 и p^4+3 такође прости.

Доказ. Разликујемо два случаја:
Ако је p = 2 онда је $p+3=5$,$p^2+3=7$,$p^3+3=11$,$p^4+3=19$ и све су то прости бројеви па је 2 једно решење.
Ако је p > 2, онда је p непаран број па је p^2 такође непаран број. Тада је p^2+3 паран, што значи и сложен.
Дакле p = 2 је једино решење. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VladimirGolub.pdf

215

Одредити све просте бројеве p за које је и број 3^p+p^3 прост.

Доказ. За p = 2 је и $3^2+2^3=17$ прост, а за друге просте бројеве p, који су уз то и непарни, збир 3^p+p^3 је збир два непарна броја, па је он паран, а тиме и сложен. Дакле,број 3^p+p^3 је прост једино за $p=2$. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VladimirGolub.pdf

216

Ако су p и $7-1$ прости бројеви онда је $7+1$ сложен број. Доказати.

Доказ. Разликујемо 2 случаја.
Ако је p $= 2$ тада је $7p - 1 = 7 \cdot 2 - 1 = 13$ такође прост број.
А број $7p + 1 = 7 \cdot 2 + 1 = 15$ је сложен, што је и требало доказати.
Ако је p > 2 онда је он и непаран па је број $7 - 1$ паран, што је у супротности са претпоставком задатка. Овде завршавамо анализу проблема, утврдили смо да тврђење важи за $p = 2$. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
`https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VladimirGolub.pdf`

217

Ако су a и n позитивни цијели бројеви при чему је $n > 1$, $n^n - 1$ прост број, доказати да је $a = 2$ и n прост број.

Доказ. Претпоставимо да n није прост број, односно да n можемо записати као производ неких простих бројева: $n = pq$.
Сада имамо да је:

$$a^n - 1 = a^{pq} - 1 = a^{p^q} - 1$$

То сада можемо раставити на сљедећи начин:

$$a^{p^q} - 1 = (a^p)^q - 1 = (a^p - 1) \cdot ((a^p)^{q-1} + (a^p)^{q-2} + ... + 1)$$

Као што видимо, број $a^n - 1$ се може записати као производ више бројева па он није прост број. Ово значи да n мора да буде прост број.

Сада узмимо да је n прост број. На основу претходног извођења видимо да број $a^n - 1$ можемо записати у облику:

$$a^n - 1 = (a - 1) \cdot (a^{n-1} + a^{n-2} + ... + 1)$$

Овакав запис би значио да $a^n - 1$ није прост број. Оно што нам смета јесте $a - 1$ које ствара производ. Да бисмо се њега ријешили, морамо ставити да је $a = 2$. Сада то можемо да замијенимо у изразу и добијамо:

$$(a - 1) \cdot (a^{n-1} + a^{n-2} + ... + 1) =$$
$$= (2 - 1) \cdot (2^{n-1} + 2^{n-2} + ... + 1) =$$
$$= 1 \cdot (2^{n-1} + 2^{n-2} + ... + 1) =$$
$$= 2^{n-1} + 2^{n-2} + ... + 1$$

Добили смо број који може да буде прост. Овим смо доказали да a мора да буде 2 да би $a^n - 1$ био прост број.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://math.dartmouth.edu/~jvoight/Sp2009-255/255-HW02.pdf`

218

Ако су p и q прости бројеви већи од 3, доказати да важи $24 \mid p^2 - q^2$.

Доказ. Ако од броја $p^2 - q^2$ одузмемо 1 и додамо 1, број се неће промијенити, а ми добијамо сљедеће:

$$p^2 - q^2 - 1 + 1 = p^2 - 1 - q^2 + 1 = (p^2 - 1) - (q^2 - 1)$$

Из овога сада треба да докажемо да важи: $24 \mid p^2 - 1$ и $24 \mid q^2 - 1$.

Даље, $p^2 - 1$ можемо записати као:

$$p^2 - 1 = (p - 1)(p + 1)$$

Како је p прост број и $p > 3$, онда имамо да су бројеви $p - 1$, p и $p + 1$ три узастопна броја. То значи да у $p - 1$ и $p + 2$ два узастопна парна броја. Из тога сиједи да је њихов прозвод дјељив са 8, односно:

$$8 \mid (p - 1)(p + 1)$$

Даље, како су $p - 1$, p и $p + 1$ три узастопна броја, то значи да је један од њих дјељив са 3. Како је p прост број, он није дјељив са 3, па то значи да је или $p - 1$ или $p + 1$ дјељив са 3, односно:

$$3 \mid p - 1$$

ili

$$3 \mid p + 1$$

Како 3 дијели један од бројева $p - 1$ и $p + 1$, и 8 дијели њихов прозвод, онда имамо да и број 24 дијели тај прозвод, па је:

$$8 \mid (p - 1)(p + 1), 3 \mid p - 1 \vee 3 \mid p + 1 \implies 24 \mid (p - 1)(p + 1)$$

Исто ово важи и за q. Овим је доказ завршен.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет из књиге Теорија бројева:
`https://www.vladimirbozovic.net/univerzitet/bozovic/wp-content/uploads/2010/01/Zbirka-rijesen`
`pdf`

219

Ако су бројеви p и $2p^2 + 1$ прости бројеви, доказати да је $3p^2 + 2$ такође прост број.

Доказ. Ако је p прост број већи од 3, тада је он облика $6 + 1$ или $6k + 5$ за неко k.
Ако је $p = 6k + 1$ онда слиједи:

$$2p^2 + 1 = 2 \cdot ((6k + 1)^2) + 1$$

А то се даље може средити уз помоћ *формуле за квадрат збира*:

$$2 \cdot ((6k+1)^2) + 1 = 2 \cdot ((6k)^2 + 2 \cdot 6k \cdot 1 + 1^2) + 1 =$$

$$= 2 \cdot (36k^2 + 12k + 1) + 1$$

То даље помножимо са 2 испред заграде и онда нађемо заједнички број за све који можемо да издвојимо:

$$2 \cdot (36k^2 + 12k + 1) + 1 = 72k^2 + 24k + 2 + 1 = 72k^2 + 24k + 3 =$$

$$= 3 \cdot (24k^2 + 8k + 1)$$

Видимо да смо добили број који је производ других бројева, па тај број није прост, што значи да наш број није облика $6k + 1$.
Сада провјеримо да ли је наш број облика $6k + 5$. Тада имамо:

$$2p^2 + 1 = 2 \cdot ((6k+5)^2) + 1$$

Па је даље:

$$2 \cdot ((6k+5)^2) + 1 = 2 \cdot ((6k)^2 + 2 \cdot 6k \cdot 5 + 5^2) + 1 =$$

$$= 2 \cdot (36k^2 + 60k + 25) + 1$$

Настављамо са сређивањем као и код провјере за претходни облик:

$$2 \cdot (36k^2 + 60k + 25) + 1 = 72k^2 + 120k + 50 + 1 = 72k^2 + 120k + 51 =$$

$$= 3 \cdot (24k^2 + 40k + 17)$$

Видимо да смо опет нијемсо добили прост број, што значи да наш број није ни облика $6k+5$.

Како наш тражени број нема ни један од поменутих облика, то значи да он није већи од 3. Дакле, остају нам само два броја, а то су 2 и 3.
Сада узмимо ове бројеве и провјеримо их у нашем изразу $2p^2 + 1$. Тада имамо:

1) $p = 2$

$$2p^2 + 1 = 2 \cdot 2^2 + 1 = 9$$

Број 9 није прост, тако да и број 2 отпада.

2) $p = 3$

$$2p^2 + 1 = 2 \cdot 3^2 + 1 = 19$$

Број 19 је прост, па број 3 задовољава наш услов.

Сада провјеравамо број 3 и за израз $3p^2 + 2$, па имамо:

$$3p^2 + 2 = 3 \cdot 3^2 + 2 = 29$$

Број 29 је прост број, па број 3 задоољава и овај услов.

Број **3** је једини број који задовољава услове задатка, па је он **једино рјешење**.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет из књиге Теорија бројева:
https://www.vladimirbozovic.net/univerzitet/bozovic/wp-content/uploads/2010/01/Zbirka-rijesen
pdf

220

Доказати да

а) $(n, 2^{2^n} + 1)$ за $n = 1, 2, ...$

б) да постоји бесконачно много цијелих бројева n таквих да $(n, 2^{2^n} + 1) > 1$ и наћи најмањи од њих

Доказ. а) Знамо да сваки дијелилац > 1 броја $F_n = 2^{2^n} + 2(1, 2, ...$ ($F-$Фермаов број) је облика $2^{n+2}k + 1$ гдје је k позитивни цијели број. Пошто за позитивне бројеве n и k важи $2^{n+2}k + 1 \geq 2^{n+2} + 1 > n$,сви дјелиоци > 1 Фермаовог броја F_n морају бити $> n$ тако да $(n, F_n = 1)$ што је и требало доказати

б) Лако можемо провјерити да је $(n, 2^n - 1) = 1$ за $n = 1, 2, 3, 4, 5$, док $(6m2^6 - 1 = 3$. За $k = 1, 2, ...,$ имамо $3 \mid 2^6 - 1 \mid 2^{6k} - 1$ тако да $(6k, 2^{6k} - 1 \geq 3$ за $k = 1, 2, ...$ Најмањи такав број је $n = 6$

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%
20-%20Sierpinski%20(1970).pdf

4 Разни задаци

Диофантове једначине, Кинеска теорема о остацима, Ојелрова ϕ функција...

221

Ријешити систем линеарних конгруенција:

$$\begin{aligned} x &\equiv 1 \pmod 7 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 9 \pmod{15} \end{aligned}$$

Доказ. Како је $m_1 = 7$, $m_2 = 4 = 2 \cdot 2$, $m_3 = 15 = 3 \cdot 5$, то су модули у паровима релативно прости, па можемо примијенити **Кинеску теорему о остацима** за решавање овог система.

$$M = m_1 \cdot m_2 \cdot m_3 = 7 \cdot 4 \cdot 15 = 420$$

$$\begin{aligned} n_1 &= \frac{M}{m_1} = \frac{420}{7} = 60 \\ n_2 &= \frac{M}{m_2} = \frac{420}{4} = 105 \\ n_3 &= \frac{M}{m_3} = \frac{420}{15} = 28 \end{aligned}$$

Да бисмо дошли до решења система, неопходно је да ријешимо следеће три линеарне конгруенције:

$$\begin{aligned} 60x_1 &\equiv 1 \pmod 7 \\ 105x_2 &\equiv 3 \pmod 4 \\ 28x_3 &\equiv 9 \pmod{15} \end{aligned}$$

Када скратимо конгруенције по одговарајућим модулима ($60 \equiv 4 \pmod 7$, $105 \equiv 1 \pmod 4$),

$28 \equiv 13 \pmod{15}$), добијамо следеће конгруенције:

$$\begin{aligned} 4x_1 &\equiv 1 \pmod 7 \\ x_2 &\equiv 3 \pmod 4 \\ 13x_3 &\equiv 9 \pmod{15} \end{aligned}$$

Када ријешимо сваку конгруенцију посебно, добијамо следеће

$$\begin{aligned} x_1 &\equiv 2 \pmod 7 \\ x_2 &\equiv 3 \pmod 4 \\ x_3 &\equiv 3 \pmod{15} \end{aligned}$$

Сада је решење полазног система:

$$\begin{aligned} x &\equiv n_1 \cdot x_1 + n_2 \cdot x_2 + n_3 \cdot x_3 \pmod M \\ &\equiv 60 \cdot 2 + 105 \cdot 3 + 28 \cdot 3 \pmod{420} \\ &\equiv 519 \pmod{420} \\ &\equiv 99 \pmod{420} \end{aligned}$$

□

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://elib.mi.sanu.ac.rs/files/journals/mk/7/mkn7p27-36.pdf`

222

Ријешити систем линеарних конгруенција

$$\begin{aligned} 11x &\equiv 13 \pmod{20} \\ 9x &\equiv 17 \pmod{25} \end{aligned}$$

Доказ. Прво ћемо ријешити $11x \equiv 13 \pmod{20}$. Примијетимо да је

$$\begin{aligned} 11 \cdot 11 = 121 &\equiv 1 \pmod{20} \\ \implies x = 13 \cdot 11 \equiv 143 &\equiv 3 \pmod{20}. \end{aligned}$$

Након тога решавамо $9x \equiv 17 \pmod{25}$. Примијетимо да је

$$\begin{aligned} 9 \cdot 11 = 99 &\equiv -1 \pmod{25} \\ \implies x = -17 \cdot 11 \equiv 8 \cdot 11 = 88 &\equiv 13 \pmod{25}. \end{aligned}$$

На овај начин добијамо да је почетни систем еквивалентан са:

$$\begin{aligned} x &\equiv 3 \pmod{20} \\ x &\equiv 13 \pmod{25} \end{aligned}$$

Како је прва конгруенција еквивалентна са $x \equiv 3 \pmod{20}$, можемо направити смјену $x = 3 + 20k$ и ставити је у другу конгруенцију. На тај начин добијамо:

$$\begin{aligned} 9(3 + 20k) &\equiv 17 \pmod{25} \\ \implies 5k &\equiv -10 \pmod{25}, \end{aligned}$$

које за решење има $k = 3, x = 3 + 20 \cdot 3 = 63$. Након проналаска једног решења, тада је због $\text{нзс}(25, 20) = 100$, опште решење дато са

$$x \equiv 63 \pmod{100}.$$

□

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/TOB02.pdf`

223

Потребан и довољан услов да линеарна Диофантова једначина $ax+by = c$ (a, b и c су цијели бројеви и $ab \neq 0$) има решење је да је број c дјељив са $\text{нзд}(a, b)$.

Доказ. Нека је $\text{нзд}(a, b) = d (d \neq 1)$. Ако је (x_0, y_0) једно цјелобројно решење линеарне Диофантове једначине $ax + by = c$, тада је $ax_0 + by_0 = c$. Тада постоје узајамно прости цијели бројеви k и l, такви да је $a = kd$ и $b = ld$. Значи да је

$$kdx_0 + ldy_0 = c,$$

тј.

$$d(kx_0 + ly_0) = c.$$

Лијева страна једнакости је дјељива са d, па мора бити и десна, тј. $d \mid c$.

Обрнуто, нека је $d \mid c$. Тада постоји цио број m, такав да је $c = md$. Како се број d може представити као хомогена линеарна функција од a и b, то је

$$d = \alpha a + \beta b (\alpha \in \mathbb{Z}, \beta \in \mathbb{Z}).$$

Тада је

$$c = md = m(\alpha a + \beta b) = a(m\alpha) + b(m\beta),$$

па је $x = m\alpha, y = m\beta$ једно решење дате једначине. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/6.%20LINEARNA%20DJ.pdf`

224

Испитати да ли линеарна Диофантова једначина $247x + 91y = 39$ има решење. Уколико има, одредити опште решење.

Доказ. Прво ћемо провјерити да ли нзд$(247, 91) \mid 39$. Дакле, тражимо нзд$(27, 59)$.

$$\begin{aligned} 247 &= 2 \cdot 91 + 65 \\ 91 &= 1 \cdot 65 + 26 \\ 65 &= 2 \cdot 26 + 13 \\ 26 &= 2 \cdot 13 \end{aligned}$$

Дакле, нзд$(247, 91) = 13$, а $13 \mid 39$, па једначина има решење. Сада тражимо опште решење:

$$x = \frac{39}{13}x_0 + \frac{91}{13}t \implies x = 3x_0 + 7t, t \in \mathbb{Z}, \tag{4.1}$$

$$y = \frac{39}{13}y_0 - \frac{247}{13}t \implies y = 3y_0 - 19t, t \in \mathbb{Z} \tag{4.2}$$

Постоје x_0 и y_0 из скупа цијелих бројева и тражимо их користећи Еуклидов алгоритам. Имамо да је $247x_0 + 91y_0 = 13$.

$$\begin{aligned} 13 = 65 - 2 \cdot 26 &= 65 - 2 \cdot (91 - 1 \cdot 65) = 65 - 2 \cdot 91 + 2 \cdot 65 \\ &= 3 \cdot 65 - 2 \cdot 91 = 3 \cdot (247 - 2 \cdot 91) - 2 \cdot 91 \\ &= 3 \cdot 247 - 8 \cdot 91 \implies x_0 = 3, y_0 = -8 \end{aligned}$$

Сада из (4.1) и (4.2) слиједи да је

$$x = 3 \cdot 3 + 7t = 9 + 7t, t \in \mathbb{Z}$$

и

$$y = 3 \cdot (-8) - 19t = -24 - 19t, t \in \mathbb{Z},$$

што је и тражено опште решење. □

(**Катарина Синђић 36/19 Д**) задатак преузет са вјежби из предмета Математика 5.

225

(а) Одредити све природне бројеве n за које је $\phi(n)$ непаран број.
(б) Одредити $\phi(1111)$.
(в) Одредити број прирпдних бројева који су релативно прости са бројем 10^{100} и мањи су од њега.

Доказ. Из дефиниције Ојлерове функције знамо да је $\phi(1) = 1$, па је $\phi(2) = 1$, јер

$$\phi(n) = n \cdot \prod_{i=1}^{k}(1 - \frac{1}{p_i})$$

је Ојлерова функција, одакле смо и закључили да је $\phi(2) = 2 \cdot (1 - \frac{1}{2}) = 1$. Претпоставимо да је $n > 2$. Ако постоји непаран фактор p_i од n, онда је $p_i - 1$ паран број, па је ϕ паран број због следће формуле:

$$\phi = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{k}(1 - \frac{1}{p_i})$$

из које добијамо да ће у једном чиниоцу функције $\phi(n)$ бити $\frac{p_i - 1}{p_i}$. Ако не постоји непаран фактор p_i од n, онда је $n = 2^{\alpha}$, $\alpha \geq 2$, па је

$$\phi(n) = 2^{\alpha - 1}(2 - 1) = 2^{\alpha - 1}.$$

Како је $\alpha - 1 \geq 1$, слиједи да је $\phi(n)$ паран број. Закључујемо да је $\phi(n)$ непаран број само за $n \in \{1,2\}$.

(б) Имамо да је $1111 = 11 \cdot 101$. Примјеном својства да је Ојлерова функција мултипликативна и чињенице да су 11 и 101 прости бројеви, добијамо:

$$\phi(1111) = \phi(11 \cdot 101) = \phi(11) \cdot \phi(101) = 10 \cdot 100 = 10000.$$

(в) Потребно је одредити $\phi(10^{100})$. Број 10^{100} можемо записати као $2^{100} \cdot 5^{100}$. Како Ојлерова функција има својство мултипликативности, можемо записати следеће:

$$\phi(10^{100}) = \phi(2^{100}5^{100}) = \phi(2^{100}) \cdot \phi(5^{100}) = 2^{99} \cdot 1 \cdot 5^{99} \cdot 4 = 4 \cdot 10^{99}.$$

□

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://e.math.hr/Vol31/Bokun#e10`

226

(а) Покажимо да постоји бесконачно много позитивних цијелих бројева n, таквих да је $\phi(n) = \frac{n}{3}$.
(б) Ако је n сложен природан број, тада је $\phi(n) \leq n - \sqrt{n}$.
(в) За сваки природан број m, постоји коначно много природних бројева n, таквих да је $\phi(n) = m$.

Доказ. (а) За све $n = 2 \cdot 3^m, m \in \mathbb{N}$, важи:

$$\phi(n) = \phi(2 \cdot 3^m) = \phi(2) \cdot \phi(3^m) = 1 \cdot 3^{m-1} \cdot (3-1) = 2 \cdot 3^{m-1} = \frac{n}{3}.$$

Чиме је доказ завршен.

(б) Будући да је n сложен природан број, n има прост фактор $p_j \leq \sqrt{n}$. Сада имамо:

$$\phi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}) \leq (1 - \frac{1}{p_j}) \leq n(1 - \frac{1}{\sqrt{n}}) = n - \sqrt{n}.$$

(в) Ако нека потенција простог броја p дијели n, тј. $p^\alpha \mid n$, и на основу својства да ако $d \mid n$, онда $\phi(d) \mid \phi(n)$, важи да

$$p^{\alpha-1}(p-1) \mid \phi(n) = m.$$

Него, онда је

$$p^\alpha \leq \frac{mp}{p-1} \leq 2m.$$

Како постоји само коначно много бројева p^α, таквих да је $p^\alpha \leq 2m$, постоји и коначно много продуката таквих потенција простих бројева. Самим тим, постоји и коначно много природних бројева са датим својством. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://e.math.hr/Vol31/Bokun#e10`

227

За све природне бројеве $n, n \neq 2, 6$, важи да је $\phi(n) \geq \sqrt{n}$.

Доказ. За $p = p^m$, гдје је p прост број и $m \geq 2$, важи да је $\frac{m}{2} \leq m - 1$, па слиједи

$$\phi(n) = p^{m-1}(p-1) \geq p^{m-1} \geq \sqrt{p^m} = \sqrt{n}. \tag{4.3}$$

У случају када је $p \neq 2$, важи и

$$\phi(n) = p^{m-1}(p-1) \geq p^{m-1}\sqrt{2} \geq \sqrt{2p^m} = \sqrt{2n}. \tag{4.4}$$

Нека је $n = p$, $p \geq 3$, гдје је p прост број. Ријешићемо квадратну функцију $f(x) = x^2 - x - 1$.

$$x_{1,2} = \frac{1 \pm \sqrt{1+4}}{2}$$
$$x_{1,2} = \frac{1 \pm \sqrt{5}}{2}$$

Можемо видјети да је квадратна функција позитивна за $x > \frac{1+\sqrt{5}}{2}$. Када замијенимо $x = \sqrt{t}$, добијамо да за $t > (\frac{1+\sqrt{5}}{2})^2$ важи $\sqrt{t} < t - 1$. Дакле, за $p \geq 3$ важи $\sqrt{p} < p - 1$, па је

$$\phi(n) = p - 1 > \sqrt{p} = \sqrt{n}. \tag{4.5}$$

За $p \geq 5$ аналогно се може показати да је

$$\phi(n) = p - 1 > \sqrt{2p} = \sqrt{2n}. \tag{4.6}$$

Ако је n непаран или ако $4 \mid n$, из (4.3) и (4.5) слиједи

$$\phi(n) = \phi(p_1^{\alpha_1}) \dots \phi(p_k^{\alpha_k}) \geq \sqrt{p_1^{\alpha_1}} \dots \sqrt{p_k^{\alpha_k}} = \sqrt{n}.$$

Ако је $n = 2k$, гдје је k непаран број, тада за $n \neq 6$ слиједи да $9 \mid k$ или k има барем један прост фактор $p \geq 5$. Из (4.4) и (4.6) слиједи

$$\phi(n) = \phi(k) \geq \sqrt{2k} = \sqrt{n},$$

чиме је доказ завршен. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`http://e.math.hr/Vol31/Bokun#e10`

228

Све примитивне Питагорине тројке (x, y, z) у којима је y паран, дате су формулом

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2,$$

гдје је $m > n$ и m, n су релативно прости природни бројеви различите парности.

Доказ. Прво ћемо дати једну дефиницију и тврђење који нам могу помоћи у овом и наредним задацима.

Дефиниција: Уређену тројку природних бројева (x, y, z), називамо Питагорина тројка ако су x и y катете, а z хипотенуза неког правоуглог троугла, тј. ако важи

$$x^2 + y^2 = z^2. \tag{4.7}$$

Ако су x, y, z релативно прости, онда кажемо да је (x, y, z) примитивна Питагорина тројка. Такав троугао називамо примитивни Питагорин троугао.

Тврђење: У свакој примитивној Питагориној тројки, тачно је један од бројева x и y непаран. Заиста, ако би x и y били парни, онда тројка не би била примитивна, а ако би x и y били непарни, онда би из $x^2+y^2 \equiv 2 \pmod 4$ и $z \equiv 0 \pmod 4$, добили контрадикцију.

Сада можемо прећи на доказ. Једначину (4.7) можемо записати у облику $y^2 = (z+x)(z-x)$. Нека је $y = 2c$, Бројеви $z+x$ и $z-x$ су парни, па постоје природни бројеви a и b, такви да је $z+x = 2a, z-x = 2b$. Сада је

$$c^2 = ab.$$

Из $z = a+b, x = a-b$, које добијамо решавањем система $z+x = 2a, z-x = 2b$, закључујемо да је $(a,b) = 1$, па постоје $m, n \in \mathbb{N}, (m,n) = 1$, такви да је $a = m^2, b = n^2$. Одавде је

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2 \tag{4.8}$$

Бројеви m и n морају бити различите парности јер је број $x = m^2 - n^2$ непаран. Бројеви x, y, z дефинсани са (4.8) задовољавају једначину (4.7). Заиста,

$$(m^2-n^2)^2 + (2mn)^2 = (m^2+n^2)^2 = m^4 + 2m^2n^2 + n^4 = (m^2+n^2)^2.$$

Треба још провјерити да су релативно прости. Претпоставимо да је $(x,z) = d > 1$. Тада је d непаран. Дакле,

$$d \mid (m^2+n^2) + (m^2-n^2) = 2m^2,$$
$$d \mid (m^2+n^2) - (m^2-n^2) = 2n^2.$$

Међутим, ово је у контрадикцији да су m и n, па самим тим и m^2 и n^2, релативно прости. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

229

Нађимо све Питагорине троуглове у којима је једна страница једнака
(а) 39
(б) 1999

Доказ. (а) Из претходног задатка имамо да су све Питагорине тројке дате идентитетом

$$[d(m^2-n^2)]^2 + (2dmn)^2 = [d(m^2+n^2)]^2.$$

У овом случају имамо три могућности, односно да је $d = 1, d = 3, d = 13$.

$$d = 1 \implies m^2+n^2 \neq 39, \text{ па мора бити } m^2-n^2 = (m-n)(m+n) = 39$$

Одавде је $m-n = 1, m+n = 39$ или $m-n = 3, m+n = 13$, што повлачи да је $m = 20, n = 19$ или $m = 8, n = 5$. На тај начин добијамо Питагорине тројке $(39, 760, 761)$ и $(39, 80, 89)$.

$$d = 3 \implies m^2-n^2 = 13 \text{ или } m^2+n^2 = 13 \implies m = 7, n = 6 \text{ или } m = 3, n = 2\ .$$

Добијене Питагорине тројке у овом случају су $(39, 252, 255)$ и $(15, 36, 39)$.

$$d = 13 \implies m^2 - n^2 = 3. \text{ Одавде је } m = 2, n = 1.$$

Дакле, у овом случају добијена Питагорина тројка је $(39, 52, 65)$.

(б) Сада је $d = 1$, па из $m^2 - n^2 = 1999$ слиједи да је $m = 1000, n = 999$, па је добијена Питагорина тројка $(1999, 1998000, 1998001)$. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

230

Једначина $x^4 + y^4 = z^2$, нема решења у скупу природних бројева, односно не постоји правоугли троугао којем су дужине катета квадрати природних бројева.

Доказ. Претпоставимо да такав троугао постоји и изаберимо међу свим таквим троугловима онај са најмањом хипотенузом. На тај начин добијамо Питагорину тројку (x^2, y^2, z). Покажимо да су x и y релативно прости. У супротном би било $x = a \cdot d, y = b \cdot d, d > 1$. Замијенимо x и y у $x^4 + y^4 = z^2$. Добијамо $z^2 = d^4(a^4 + b^4)$, одакле слиједи да постоји $c \in \mathbb{N}$, такав да је $z^2 = d^2 \cdot c$. На тај начин добијамо Питагорину тројку (a^2, b^2, c) са хипотенузом мањом од z, што је контрадикција.

Дакле, (x^2, y^2, z) је примитивна Питагорина тројка, па из теореме која је доказана у неком од претходних задатака (ако одаберемо да је y паран), која гласи:

све примитивне Питагорине тројке (x, y, z) у којима је y паран, дате су формулом

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2,$$

гдје је $m > n$ и m, n су релативно прости природни бројеви различите парности,

слиједи да постоје релативно прости природни бројеви m, n различите парности, тако да важи:

$$x^2 = m^2 - n^2, y^2 = 2mn, z = m^2 + n^2.$$

Из $x^2 + n^2 = m^2$ слиједи да је n паран, а m непаран. Ставимо $n = 2k, y = 2t$, па добијамо:

$$t^2 = mk \implies \exists r, s \in \mathbb{N},$$

такви да је $m = r^2, k = s^2$. Будући да је (x, n, m) примитивна Питагорина тројка, по горе наведеној теореми, постоје u, v, такви да је $(u, v) = 1, n = 2uv, m = u^2 + v^2$. Сада из $n = 2s^2$ слиједи $s^2 = uv$, па постоје $a, b \in \mathbb{N}$, такви да је $u = a^2, v = b^2$. Према томе, $a^4 + b^4 = r^2$, па је (a^2, b^2, r) Питагорина тројка за чију хипотенузу важи: $r < r^2 = m < m^2 + n^2 = z$, што је у супротности с минималношћу од z. □

(**Катарина Синђић 36/19 Д**) задатак преузет са
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

231

Ријешити систем линеарних конгруенција користећи Кинеску теорему о остацима:

$$\begin{aligned} x &\equiv 10 \pmod{12}, \\ x &\equiv 8 \pmod{15}, \\ x &\equiv 6 \pmod{56}. \end{aligned}$$

Доказ. Након поступка описаног у претходном примјеру добијамо:

$$\begin{aligned} x &\equiv 2 \pmod{2^2}, x \equiv 6 \pmod{2^3}, \\ x &\equiv 1 \pmod{3}, x \equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5}, x \equiv 6 \pmod{7}. \end{aligned}$$

Како неки број при дијељењу са 3 не може истовремено дати остатак 1 и 2, закључујемо да дати систем нема рјешења. □

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://elib.mi.sanu.ac.rs/files/journals/mk/7/mkn7p27-36.pdf`

232

Кинеска теорема о остацима: Нека су $m_1, m_2, \ldots, m_r$ у паровима релативно прости природни бројеви и нека су $a_1, a_2, \ldots a_r$ цијели бројеви. Тада систем од r конгруенција

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

има решење. Ако је x_0 једно решење, онда су сва решења тог система дата са

$$x \equiv x_0 \pmod{m_1 m_2 \ldots m_r}.$$

Доказ. Нека је $M = m_1 m_2 \ldots m_r$ и нека је $n_j = \frac{M}{m_j}$ за $j = 1, 2, \ldots r$. Тада је нзд$(m_j, n_j) = 1$, па постоји цијели број x_j, такав да је $n_j x_j \equiv a_j \pmod{m_j}$. Сада за број

$$x_0 = n_1 x_1 + n_2 x_2 + \ldots n_r x_r$$

значи да

$$x_0 \equiv 0 + 0 + \cdots + n_j x_j + 0 + \ldots 0 \equiv a_j \pmod{m_j}$$

па слиједи да је x_0 решење датог система конгруенција. Ако су x и y два решења датог система конгруенција, онда је $x \equiv y \pmod{m_j}$ за $j = 1, 2, \ldots, r$, па како су m_j у паровима прости, добијамо да је $x \equiv y \pmod{M}$. □

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/BIN01.pdf`

233

Ријешити систем линеарних конгруенција преко Кинеске теореме са остацима:

$$\begin{aligned} 7x &\equiv 12 \pmod{39}, \\ 2x &\equiv 7 \pmod{35}, \\ 21x &\equiv 15 \pmod{22}. \end{aligned}$$

Доказ. Иако су модули у паровима релативно прости,за примјену Кинеске теореме о остацима проблем нам праве лијеве стране конгруенција. Како је нзд$(7, 2, 21) = 42$, то прву конгруенцију множимо са 6=42/7, другу множимо са 21=42/2, а трећу са 2=42/12 и добијамо следећи систем:

$$\begin{aligned} 42x &\equiv 72 \pmod{234}, \\ 42x &\equiv 147 \pmod{735}, \\ 42x &\equiv 30 \pmod{44}. \end{aligned}$$

Уводећи супституцију t = 42x, добијамо систем:

$$\begin{aligned} t &\equiv 72 \pmod{234}, \\ t &\equiv 147 \pmod{735}, \\ t &\equiv 30 \pmod{44}. \end{aligned}$$

Ријешимо ли га на већ описани начин, добијамо да је

$$t = 71442 \pmod{1261260}.$$

Вратимо ли супституцију назад, добијамо да је рјешење полазног система:

$$x = 1701 \pmod{30030}.$$

□

(**Ива Вучићевић 18/17 Д**) задатак преузет са
`http://elib.mi.sanu.ac.rs/files/journals/mk/7/mkn7p27-36.pdf`

234

Колико има парова природних бројева (x, y) таквих да је $4x + 7 = 2005$?

Доказ. У овој једначини видимо да 2005 није дјељив са 4. Како је $4x = 2005 - 7y$, видимо да $2005 - 7y$ мора бити дјељив са 4.

$$\begin{aligned} y = 0 &\Rightarrow 2005 - 0 = 2005 \\ y = 1 &\Rightarrow 2005 - 7 = 1998 \\ y = 2 &\Rightarrow 2005 - 14 = 1991 \\ y = 3 &\Rightarrow 2005 - 21 = 1894 \end{aligned}$$

Дакле, добијамо да само за $y = 3 \Rightarrow 2005 - 21 = 1894$ је дјељив са 4. Тј. $1894 : 4 = 496$, па наше почетно решење можемо записати као $(x_0, y_0) = (496, 3)$, јер је:

$$\begin{aligned} 4 \cdot x + 7 \cdot y &= 2005 \\ 4 \cdot 496 + 7 \cdot 3 &= 2005. \end{aligned}$$

Како је $4x + 7y = 2005$, имамо следеће:

$$\begin{aligned} x &= x_0 - b_k \\ x &= 496 - 7k \\ 496 - 7k &> 0 \\ 7k &< 496 \\ k &\leq 70 \end{aligned} \qquad \begin{aligned} y &= y_0 + ak \\ y &= 3 + 4k \\ 3 + 4k &> 0 \\ 4k &> -3 \\ k &\geq 0 \end{aligned}$$

Односно имамо:

$$0 \geq k \leq 70$$

Постоји тачно 71 решење, тј. постоји тачно 71 уређени пар који задовољава ову једначину. □

(**Ива Вучићевић 18/17Д**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/6.%20LINEARNA%20DJ.pdf`

235

Наћи партикуларно и опште решење Диофантове једначине
$1000x - 123y = 5$.

Доказ.

$$1000 = 123 \cdot 8 + 16$$
$$123 = 16 \cdot 7 + 11$$
$$16 = 11 \cdot 1 + 5$$
$$11 = 5 \cdot 2 + 1$$
$$5 = 1 \cdot 5$$

Видимо да дата једначина има решење јер $1 = (1000, 123), 1|5$.
$1 = 11 - 5 \cdot 2 = 11 - (16 - 11) \cdot 2 = 3 \cdot 11 - 2 \cdot 16 = 3(123 - 16 \cdot 7) - 2 \cdot 16 = 3 \cdot 123 - 23 \cdot 16 = 3 \cdot 123 - 23(1000 - 123 \cdot 8) = -23 \cdot 1000 + 187 \cdot 123 = -23 \cdot 1000 - 187 \cdot (-123)$
Дакле, $\alpha = -23, \beta = -187, q = 5$.
Партикуларна решења:
$x_0 = -23 \cdot 5 = -115, y_0 = -187 \cdot 5 = -935$
Општа решења:
$x = -115 + 123t, y = -935 + 1000t$. □

(**Ива Вучићевић 18/17Д**) задатак преузет са
`https://www.scribd.com/document/375050244/Teorija-brojeva-radna-verzija-pdf`

236

Воз има 12 вагона. Сваки вагон има исти број купеа. Марко путује у трећем вагону, у 18. купеу. Ивана путује у 7. вагону, у 50. купеу. Колико купеа има сваки караван?

Доказ. Означити са x број купеа у сваком вагону. Тада је $2x + y = 18$ и $50 = 6x + z$, гдје је y редни број купеа у трећем вагону где се налази Марко, а z је редни број купеа у 7. вагону гдје се налази Ивана. Очигледно су x, y и $z \in N$, а y и z су мањи од x. Имамо:

$$y = 18 - 2x, z = 50 - 6x$$

из чега слиједи да је:

$$y = 18 - 2x < x, z = 50 - 6x < x,$$

односно:

$$x > 7.$$

За $x = 8$ добијамо да су $y = 2$ и $z = 2$. За $x > 8$, y и z нису природни бројеви (тј. мањи су од 0) па закључујемо да је једино решење $x = 8$, односно да сваки вагон има 8 купеа.

□

(**Ива Вучићевић 18/17Д**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

237

Одредити остатак при дијељењу броја 2017^{10^6} са 55.

Доказ. Како је $\phi(55) = \phi(5)\ \phi(11) = 40$ и $(2017{,}55) = 1$, из Ојлерове теореме слиједи:

$$2017^{40} \equiv 1 \pmod{55}.$$

Онда је,

$$2017^{10^6} \equiv 2017^{40 \cdot 25000} \equiv 1 \pmod{55}.$$

Па је тражени остатак 1. □

(**Ива Вучићевић 18/17Д**) задатак преузет са
`http://e.math.hr/Vol31/Bokun`

238

Одредити три последње цифре у децималном запису броја 3^{4004}.

Доказ. Уочимо да решење можемо добити одређивањем остатка при дијељењу датог броја са 1000. Будући да је $\phi(1000) = \phi(2^3)\phi(5^3) = 400$ и $(3{,}1000) = 1$ примјеном Ојлерове теореме добијамо:

$$3^{400} \equiv 1 \pmod{1000},$$

одатле слиједи:

$$3^{4004} \equiv 3^{400 \cdot 10 + 4} \equiv 3^4 \equiv 81 \pmod{1000}.$$

Закључујемо да су задње три цифре броја 3^{4004} једнаке 081. □

(**Ива Вучићевић 18/17Д**) задатак преузет са
`http://e.math.hr/Vol31/Bokun`

239

Ако су n и p природни бројеви и p прост број, тада је:

$$\phi(p^n) = p^{n-1} = p^n(1 - \frac{1}{p}).$$

Доказ. Сваки од природних бројева од 1 до p^n или је дељив са p или је узајамно прост са p. Број оних који су дељиви са p једнак је p^{n-1}. Дакле, оних који су релативно прости са p, према томе и са p^n, има p^n - $p^{n-1} = p^n(1 - \frac{1}{p})$. □

(**Ива Вучићевић 18/17Д**) задатак преузет са
`https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic`
`pdf`

240

Колико парова троцифрених природних бројева $(x\ ,\ y)$ задовољава услов $15x + 3y = 2010$?

Доказ. Након дијељења задате једначине са 3, добићемо

$$5x + y = 670.$$

Тада је $y = 670 - 5x$. Како су x и y троцифрени природни бројеви, имамо:

$$100 \leq x < 1000, 100 \leq y < 1000,$$

односно

$$100 \leq 670 - 5x < 1000,$$

то јест

$$114 \geq x > 66.$$

Како је x троцифрен слиједи:

$$100 \leq x \leq 114 \tag{4.9}$$

што значи да 15 парова троцифрених природних бројева $x\ ,\ y)$ задовољава једначину $15x + 3y = 2010$. (Троцифрена решења дате једначине у скупу природних бројева су ((100, 170), (101, 165), (102, 160), ..., (113, 105), (114, 100).)

[2. начин] Лако је видети да је партикуларно решење једначине $5x + y = 670$ уређени пар (1,665). Из тога следи да су дата сва решења почетне једначине као

$$s(1 + t, 665 - 5t), t \in Z.$$

Док тражимо парове троцифрених бројева, имамо:

$$100 \leq 1 + t \leq 999, 100 \leq 665 - 5t \leq 999$$

из чега произлази да је $t \in [99, 113] \cap Z$. Дакле, имамо 15 троцифрених парова природних бројева који задовољавају почетни услов. □

(**Ива Вучићевић 18/17Д**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

241

Познато је да постоје тачно два проста броја чије реципрочне вредности записане у облику децималног броја имају периоде 7.
Један од тих бројева је 4649. Који је други?

Доказ. Нека је p тражени број. Тада је

$$\frac{1}{p} = 0, a_1 a_2 \dots a_n (b_1 b_2 \dots b_7).$$

Из тога следи да је

$$\begin{aligned} q &= 10^{n+7} \cdot \frac{1}{p} - 10^n \cdot \frac{1}{p} \\ &= \overline{a_1 a_2 \dots a_n b_1 b_2 \dots b_7,} (b_1 b_2 \dots b_7) - \overline{a_1 a_2 \dots a_n,} (b_1 b_2 \dots b_7) \\ &= \overline{a_1 a_2 \dots a_n b_1 b_2 \dots b_7} - \overline{a_1 a_2 \dots a_n} \end{aligned}$$

цео број. Дакле,

$$10^n \cdot (10^7 - 1) \cdot \frac{1}{p} = 10^n \cdot 9999999 \cdot \frac{1}{p} = q,$$

одакле је

$$p = \frac{10^n \cdot 9999999}{q} = \frac{2^n \cdot 5^n \cdot 3^2 \cdot 239 \cdot 4649}{q}.$$

Како је p прост број, q је производ неких од наведених фактора. Другим речима, $p \in \{2, 3, 5, 239, 4649\}$. Могућност $p = 4649$ отпада због услова задатка. Такође отпадају $p = 2, 3, 5$, јер њихове реципрочне вредности немају периоде 7; $\frac{1}{2} = 0,5$, $\frac{1}{3} = 0,(3)$, $\frac{1}{5} = 0,2$. Тако остаје $p = 239$, што и јесте решење с обзиром на то да је $\frac{1}{239} = 0,(0041841)$. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са `https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf`

242

Низ $a_n, n \in N$, природних бројева задат је на следећи начин:
$a_1 = 200, a_2 = 1$ и $a_{n+2} =$ остатак при дељењу збира $a_n + a_{n+1}$ са $102, n \in N$.
Одредити остатак при дељењу броја $a_1^3 + a_2^3 + \dots + a_{2005}^3$ са 9,

Доказ. Није тешко показати да важе следеће импликације:

$$\begin{aligned} a \equiv b \pmod{102} &\Rightarrow a \equiv b \pmod{3}; \\ a \equiv b \pmod{3} &\Rightarrow a^3 \equiv b^3 \pmod{9}. \end{aligned}$$

Како је, према услову задатка, за сваки природан број n,

$$a_{n+2} \equiv a_n + a_{n+1} \pmod{102},$$

то је и

$$a_{n+2} \equiv a_n + a_{n+1} \pmod{3},$$

па је:

$$a_1 \equiv -1 \pmod 3, \quad a_2 \equiv 1 \pmod 3, \quad a_3 \equiv 0 \pmod 3,$$
$$a_4 \equiv 1 \pmod 3, \quad a_5 \equiv 1 \pmod 3, \quad a_6 \equiv -1 \pmod 3,$$
$$a_7 \equiv 0 \pmod 3, \quad a_8 \equiv -1 \pmod 3.$$

Како је

$$\begin{aligned} a_{n+4} &\equiv a_{n+3} + a_{n+2} \equiv (a_{n+2} + a_{n+1}) + a_{n+2} \\ &\equiv 2a_{n+2} + a_{n+1} \equiv 2(a_{n+1} + a_n) + a_{n+1} \\ &\equiv 3a_{n+1} + 2a_n \equiv -a_n \pmod 3, \end{aligned}$$

то је $a_{n+8} \equiv -a_{n+4} \equiv a_n \pmod 3$, па је

$$a_{8m+k} \equiv a_K \pmod 3, \qquad (k = 1, 2, \ldots, 8).$$

Сада имамо да је

$$\begin{aligned} &a_{8m+1}^3 + a_{8m+2}^3 + \cdots + a_{8m+8}^3 \\ &\equiv a_1^3 + a_2^3 + \cdots + a_8^3 \\ &\equiv (-1)^3 + 1^3 + 0^3 + 1^3 + 1^3 + (-1)^3 + 0^3 + (-1)^3 \\ &\equiv 0 \pmod 9. \end{aligned}$$

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са `https://www.scribd.com/document/375892874/Zbirka-rijesenih-zadataka-iz-teorije-brojeva-Nebojsa-Ikodinovic-pdf`

243

Ако је $\{r_1, r_2, \ldots, r_m\}$ потпун систем остатака по *modulu* $m, a \in N$ и $(a, m) = 1$, тада је $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ такође потпун систем остатака *modulu* m за произвољан цели број b.

Доказ. На основу *дефиниције* јасно је да је овде треба доказати да ниједан од та два елемнта скупа $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ нису конгруентна по *modulu* m.
Ако би били конгруентни, тј. ако би било

$ar_i + b \equiv ar_j + b \pmod m$ за неке $i, j \in \{1, 2, \ldots, m\}$ и $i \neq j$, тада на основу *теореме* следи $ar_i \equiv ar_j \pmod m$,а како је $(a, m) = 1$ даље следи $r_i \equiv r_j \pmod m$.

Међутим $r_i \equiv r_j \pmod{m}$ повлачи да скуп $\{r_1, r_2, \ldots, r_m\}$ није потпун систем остатака по *modulu* m што је немогуће.
Дакле, ниједан од два елемента скупа $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ нису конгруентна, па стога они чине потпун систем остатака по *modulu* m, што је и требало доказати.

Дефиниција
Скуп целих бројева $\{r_1, r_2, \ldots, r_m\}$ зове се **потпуни систем остатака по** *modulu* m ако се за сваки $x \in Z$ постоји тачно један r_j такав да је $x \equiv r_j \pmod{m}$.

Теорема
Нека су $a, b, c \in Z$ и нека је $a \equiv b \pmod{m}$. Тада вреди:

1. $a + b \equiv b + c \pmod{m}$
2. $a - c \equiv b - c \pmod{m}$
3. $ac \equiv bc \pmod{m}$.

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

244

Решити у скупу N једначину

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{pq},$$

p, q прости бројеви ($p, q \in Z$).

Доказ.

$$\begin{aligned} \frac{x+y}{xy} &= \frac{1}{pq} \\ pq(x+y) &= xy \\ xy - xpq - ypq &= 0 \\ x(y-pq) - ypq &= 0 \\ x(y-pq) - pq(y-pq) &= p^2q^2 \\ (x-pq)(y-pq) &= p^2q^2 \end{aligned}$$

Како су бројеви p и q прости, једини природни делиоци од p^2q^2 су: $1, p, q, p^2, q^2, pq, p^2q, pq^2, p^2q^2$, па се разликују следеће могућности:

1. $x - pq = 1$ и $y - pq = p^2q^2$, одакле је $x = 1 + pq$ и $y = pq + p^2q^2$.

2. $x - pq = p$ и $y - pq = pq^2$, одакле је $x = p + pq$ и $y = pq + pq^2$.

3. $x - pq = q$ и $y - pq = p^2q$, одакле је $x = q + pq$ и $y = pq + p^2q$.

4. $x - pq = p^2$ и $y - pq = q^2$, одакле је $x = p^2 + pq$ и $y = pq + p^2$.

5. $x - pq = q^2$ и $y - pq = p^2$, одакле је $x = q^2 + pq$ и $y = pq + p^2$.

6. $x - pq = pq$ и $y - oq = pq$, одакле је $x = pq + pq$ и $y = pq + pq$.

7. $x - pq = p^2q$ и $y - pq = p$, одакле је $x = p^2q + pq$ и $y = pq + q$.

8. $x - pq = pq^2$ и $y - pq = p$, одакле је $x = pq^2 + pq$ и $y = pq + p$.

9. $x - pq = p^2q^2$ и $y - pq = 1$, одакле је $x = p^2q^2 + pq$ и $y = pq + 1$.

На овај начин смо добили сва (девет) решења (x, y) у скупу природних бројева. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са `https://www.academia.edu/38208976/Diofantove_jedna%C4%8Dine_-_Zbirka_zadataka_za_dodatnu_nastavu_iz_matematike`

245

Доказати да у скупу целих бројева једначина

$$5^x + 6^y = 234567$$

нема решења.

Доказ. Вреди

$$5 \equiv 0 \pmod 5 \Rightarrow 5^x \equiv 0 \pmod 5$$

за свако $x \in Z$. Очито је

$$6 \equiv 1 \pmod 5 \Rightarrow 6^y \equiv 1 \pmod 5$$

за свако $y \in Z$. Одавде следи (сабирањем претходних конгуренција) да је

$$5^x + 6^y \equiv 1 \pmod 5, \quad \forall \quad x, y \in Z. \tag{4.10}$$

Међутим, за десну страну једначине вреди

$$234567 \equiv 2 \pmod 5$$

па због (4.10) вреди

$$1 \equiv 2 \pmod 5$$

што је немогуће, па полазна једначина нема решења ни за једно $x, y \in Z$. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са `https://www.academia.edu/38208976/Diofantove_jedna%C4%8Dine_-_Zbirka_zadataka_za_dodatnu_nastavu_iz_matematike`

246

Да ли постоје природни бројеви m и n такви да вреди једнакост

$$3^m + 7^m = 8^n.$$

Доказ. Посматрајмо остатке по модулу 4. Како је $3 \equiv -1 \pmod 4$ то је

$$3^m \equiv (-1)^m \pmod 4$$

за свако $m \in N$. Даље је $7 \equiv -1 \pmod 4$ па је $7^m \equiv (-1)^m \pmod 4$ за свако $m \in N$. Одавде је

$$(\forall m \in N) \qquad 3^m + 7^m \equiv (-1)^m + (-1)^m \equiv 2 \cdot (-1)^m \pmod 4.$$

За десну страну полазне једначине вреди $8 \equiv 0 \pmod 4$ одакле је $8^2 \equiv 0 \pmod 4$ за свако $n \in N$. Одавде закључујемо, ако би полазна једначина имала решење за неке m и n онда би морало да вреди

$$2 \cdot (-1)^m \equiv 0 \pmod 4.$$

Међутим, ако је m парно, тада је

$$2 \equiv 0 \pmod 4$$

што није тачно, а ако је m непарно онда је

$$-2 \equiv 0 \pmod 4 \Leftrightarrow 2 \equiv 0 \pmod 4$$

што, очито, није тачно. Дакле, једначине нема решења ни за које m, n из скупа природних бројева. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са `https://www.academia.edu/38208976/Diofantove_jedna%C4%8Dine_-_Zbirka_zadataka_za_dodatnu_nastavu_iz_matematike`

247

У једној књижари оловка кошта 0,5 (пола) € , свеска 1 €, а књига 5 € .
На колико се начина за тачно 100 € може купити тачно 100 предмета ?
Колико од 100 купљених предмета су оловке, свеске и књиге ?

Доказ. Нека је број купљених оловки x, број свески y и број књига z. Тада је

$$x + y + z = 100,$$

јер их укупно има 100. Цена купљених предмета је

$$\frac{1}{2}2x + y + 5z = 100.$$

Две добијене једначине представљају систем Диофантових једначина са три непознате.

Ако се од прве једначине одузме друга добија се

$$\frac{1}{2}x - 4z = 0.$$

Следи да је $x = 8z$.

Тада је

$$8z + y + z = 100,$$

па је $y = 100 - 8z$.

Према томе опште решење добијеног система једначина је:

$$x = 8k; y = 100 - 9k; z = k.$$

С обзиром да је

$$0 \leqslant x = 8k \leqslant 100,$$

то је $0 \leqslant k \leqslant 12$.

Сва "реална"решења проблема дата су у следећој табели, јер теоријски проблем има бесконачно решења, али реално, у животној ситуацији свега 12:

k	0	1	2	3	4	5	6	7	8	9	10	11
x	0	8	16	24	32	40	48	56	64	72	80	88
y	100	91	82	73	64	55	46	37	28	19	10	1
z	0	1	2	3	4	5	6	7	8	9	10	11

□

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/6.%20LINEARNA%20DJ.pdf`

248

Одредити најмањи природан број који при дељењу са 6 даје остатак 4, при дељењу са 7 даје остатак 5, а при дељењу са 11 даје остатак 6.

Доказ. Дакле, треба решити систем линеарних конгруенција

$$\begin{aligned} x &\equiv 4 \pmod 6 \\ x &\equiv 5 \pmod 7 \\ x &\equiv 6 \pmod{11} \end{aligned}$$

Имамо да је $M = 6 \cdot 7 \cdot 11 = 462$.

$$\begin{aligned} M_1 &= \frac{M}{m_1} = \frac{462}{6} = 77 \\ M_2 &= \frac{M}{m_2} = \frac{462}{7} = 66 \\ M_3 &= \frac{M}{m_3} = \frac{462}{11} = 42 \end{aligned}$$

Сада треба решити следеће конгруенције:

$$\begin{aligned} 77y_1 &\equiv 1 \pmod 6 \\ 66y_2 &\equiv 1 \pmod 7 \\ 42y_1 &\equiv 1 \pmod{11} \end{aligned}$$

Њихова решења налазимо користећи Еуклидов алгоритам, уствари, тражимо решења линеарних Диофантових једначина:

$$\begin{aligned} 77y_1 - 6y_1^{'} &= 1 \\ 66y_2 - 7y_2^{'} &= 1 \\ 42y_3 - 11y_3^{'} &= 1 \end{aligned}$$

Дакле, (Еуклидов алгоритам)

$$\left\{ \begin{array}{r} 77 = 6 \cdot 12 + 5 \\ 6 = 5 \cdot 1 + 1 \end{array} \right\} 1 = 6 - 5 = 6 - (77 - 6 \cdot 12) = 13 \cdot 6 + 17 \cdot (-1), y_1 = -1.$$

$$\left\{ \begin{array}{r} 66 = 7 \cdot 9 + 3 \\ 7 = 3 \cdot 2 + 1 \end{array} \right\} 1 = 7 - 3 \cdot 2 = 7 - (66 - 7 \cdot 9) \cdot 2 = (-2) \cdot 66 + 19 \cdot 7, y_2 = -2.$$

$$\left\{ \begin{array}{r} 42 = 11 \cdot 3 + 9 \\ 11 = 1 \cdot 9 + 2 \\ 9 = 4 \cdot 2 + 1 \end{array} \right\} 1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (11 - 9) = 9 - 4 \cdot (11 - (42 - 11 \cdot 3)) = \cdots =$$

$5 \cdot 42 - 19 \cdot 11, y_3 = 5.$

Тражено решење је $x = 4 \cdot 77 \cdot (-1) + 5 \cdot 66 \cdot (-2) + 6 \cdot 42 \cdot 5 = -308 - 660 + 1260 = 292$
Дакле, $x = 292$ је решење датог система. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://www.ss-ilok.skole.hr/dokumenti?dm_document_id=104&dm_dnl=1`

249

Троје деце у породици имају стопала дужине 5 инчи, 7 инчи и 9 инчи. Када мере дужину трпезарије у њиховој кући користећи своја стопала, сваки открива да су преостала 3 инча. Колико је дугачка трпезарија ?

Доказ. Ако је n дужина трпезарије у инчима, ово можемо решити користећи Кинеску теорему о остацима:

$$\begin{aligned} n &\equiv 3 \pmod 5 \\ n &\equiv 3 \pmod 7 \\ n &\equiv 3 \pmod 9. \end{aligned}$$

Овде

$$\begin{aligned} a_1 &= 3, & a_2 &= 3, & a_3 &= 3 \\ m_1 &= 5, & m_2 &= 7, & m_3 &= 9, \end{aligned}$$

и

$$M_1 = 7 \cdot 9 = 63, \qquad M_2 = 5 \cdot 9 = 45, \qquad M_3 = 5 \cdot 7 = 35.$$

Такође, решавајући конгруенције

$$\begin{aligned} M_1 y_1 &\equiv 1 \pmod{m_1} \\ M_2 y_2 &\equiv 1 \pmod{m_2} \\ M_3 y_3 &\equiv 1 \pmod{m_3} \end{aligned}$$

за инверизије y_1, y_2 и y_3, имамо

$$y_1 \equiv 2 \pmod 5, \qquad y_2 \equiv 5 \pmod 7, \qquad y_3 \equiv 8 \pmod 9,$$

и јединствено решење по модулу $5 \cdot 7 \cdot 9$ је добијено преко

$$\begin{aligned} n &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 3 \cdot 63 \cdot 2 + 3 \cdot 45 \cdot 5 + 3 \cdot 35 \cdot 8 \\ &= 378 + 675 + 840 \\ &= 1893 \equiv 3 \pmod{315}. \end{aligned}$$

Према овоме разумљиво решење би било $n = 3 + 315 = 318$ инча, или 26 стопа и 6 инча. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://www.math.ualberta.ca/~isaac/math324/s10/soln3.pdf`

250

Ако се из корпе изваде 2,3,4,5,6, и 7 јаја истовремено, у корпи остају 1,2,3,4,5, и 0 јаја. Који је најмањи могући број јаја која су могла остати у корпи ?

Доказ. Можемо користити Кинеску теорему о остацима да решимо конгруенцију

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 0 \pmod 7 \end{aligned}$$

Одавде имамо

$$x \equiv 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 4 \cdot 42 \cdot (-2) + 0 \cdot 30 \cdot (-3) \pmod{2 \cdot 3 \cdot 5 \cdot 7}$$

па је $x \equiv -91 \pmod{210}$.Знамо да не може бити негативан број јаја у корпи. Наша Кинеска теорема о остацима нам говори да наше решење не може бити више од 210, ако погледамо класу конгруенције од -91 модул 210:

$$\{\dots, -91, 119, 329, 539, \dots\}$$

Закључијемо да је 119 најмањи позитивни остатак и да 119 задовољава све захтјеве наше конгруенције. □

(**Елмаз Фератовић 30/17 Д**) задатак преузет са
`http://zimmer.csufresno.edu/~tkelm/teaching/math116/homework/hw5soln_116_s07.pdf`

251

Ријешити систем конгруенција користећи Кинеску теорему о остацима

$$\begin{cases} x \equiv 2 \pmod 9 \\ x \equiv 4 \pmod{10} \\ x \equiv 8 \pmod{11} \end{cases}$$

Доказ. Како је $\text{нзд}(9,10) = \text{нзд}(9,11) = \text{нзд}(10,11) = 1 \Rightarrow$ дати систем има јединствено рјешење по модулу $n = 9 \cdot 10 \cdot 11 = 990$
Нека је $k_1 = 9$, $k_2 = 10$, $k_3 = 11$

Тада је:

$$M_1 = \frac{n}{k_1} = \frac{990}{9} = 110 \qquad M_2 = \frac{n}{k_2} = \frac{990}{10} = 99 \qquad M_3 = \frac{n}{k_3} = \frac{990}{11} = 90$$

Сада формирамо нови систем

$$\begin{cases} M_1y_1 \equiv 1 \pmod 9 \\ M_2y_2 \equiv 1 \pmod{10} \\ M_3y_3 \equiv 1 \pmod{11} \end{cases} \iff \begin{cases} 110y_1 \equiv 1 \pmod 9 \\ 99y_2 \equiv 1 \pmod{10} \\ 90y_3 \equiv 1 \pmod{11} \end{cases} \iff \begin{cases} 2y_1 \equiv 1 \pmod 9 \\ -y_2 \equiv 1 \pmod{10} \\ 2y_3 \equiv 1 \pmod{11} \end{cases}$$

Потребно је пронаћи по једно рјешење за сваку од конгруенција у посљедњем систему. Лако уочавамо да су $y_1 = 5,\ \ y_2 = -1,\ \ y_3 = 6$ рјешења.

Сада формирамо рјешење почетног система конгруенција

$$x_0 = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 2 \cdot 110 \cdot 5 + 4 \cdot 99 \cdot (-1) + 8 \cdot 90 \cdot 6 = 5024$$

$$\begin{gathered} x \equiv 5024 \pmod{990} \\ x \equiv 74 \pmod{990} \end{gathered}$$

Тако да сва рјешења задатог система конгруенција имају облик:

$$x = 74 + 990t\ ,\ t \in \mathbb{Z}$$

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`https://maths.ucd.ie/courses/math10040/Chapter3_13.pdf`

252

Наћи посљедње двије цифре броја $7^{7^{100}}$.

Доказ. $\phi(100) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = 40$. Па је по Ојлеровој теореми:

$$7^{40} \equiv 1 \pmod{100}$$

И како је $\phi(40) = \phi(2^3)\phi(5) = 4 \cdot 4 = 16 \Rightarrow 7^{16} \equiv 1 \pmod{100}$
Сада је $1000 = 16 \cdot 62 + 8$, па добијамо:

$$\begin{aligned} 7^{1000} &\equiv (7^{16})^{62}7^8 \pmod{40} \\ &\equiv 1^{62}7^8 \pmod{40} \\ &\equiv (7^4)^2 \pmod{40} \end{aligned}$$

Ово значи да је $7^{1000} = 1 + 40t,\ t \in \mathbb{Z}$, па задати број можемо приказати као:

$$7^{7^{100}} \equiv 7^{1+40t} \equiv 7 \cdot (7^{40})^t \equiv 7 \pmod{100}$$

Ово значи да су посљедње двије цифре задатог броја 07. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`http://www.math.toronto.edu/rosent/Mat246Y/PDF/cong.pdf`

253

Ријешити систем конгруенција користећи Кинеску теорему о остацима

$$\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 3 \pmod{10} \\ x \equiv 8 \pmod{15} \end{cases}$$

Доказ. Како бројеви $6, 10, 15$ нису узајамно прости, не можемо директно примијенити Кинеску теорему о остацима.
Наш полазни систем је еквивалентан са:

$$\begin{array}{lll} x \equiv 5 \pmod 2 & x \equiv 3 \pmod 2 & x \equiv 8 \pmod 3 \\ x \equiv 5 \pmod 3 & x \equiv 3 \pmod 5 & x \equiv 8 \pmod 5 \end{array}$$

Издвојимо конгруенције које одговарају истом простом броју

$$\begin{array}{lll} x \equiv 5 \pmod 2 & \iff & x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod 2 & \iff & x \equiv 1 \pmod 2 \end{array}$$

$$\begin{array}{lll} x \equiv 5 \pmod 3 & \iff & x \equiv 2 \pmod 3 \\ x \equiv 8 \pmod 3 & \iff & x \equiv 2 \pmod 3 \end{array}$$

$$\begin{array}{lll} x \equiv 8 \pmod 5 & \iff & x \equiv 3 \pmod 5 \\ & & x \equiv 3 \pmod 5 \end{array}$$

Сада имамо систем конгруенција

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

гдје су 2, 3, 5 у паровима релативно прости природни бројеви, па можемо примијенити Кинеску теорему о остацима.
Нека је $k_1 = 2$, $k_2 = 3$, $k_3 = 5$. И $n = k_1 \cdot k_2 \cdot k_3 = 30$

Тада је:

$$M_1 = \frac{n}{k_1} = \frac{30}{2} = 15 \qquad M_2 = \frac{n}{k_2} = \frac{30}{3} = 10 \qquad M_3 = \frac{n}{k_3} = \frac{30}{5} = 6$$

Сада формирамо нови систем

$$\begin{cases} M_1 y_1 \equiv 1 \pmod 2 \\ M_2 y_2 \equiv 1 \pmod 3 \\ M_3 y_3 \equiv 1 \pmod 5 \end{cases} \iff \begin{cases} 15 y_1 \equiv 1 \pmod 2 \\ 10 y_2 \equiv 1 \pmod 3 \\ 6 y_3 \equiv 1 \pmod 5 \end{cases} \iff \begin{cases} y_1 \equiv 1 \pmod 2 \\ y_2 \equiv 1 \pmod 3 \\ y_3 \equiv 1 \pmod 5 \end{cases}$$

Потребно је пронаћи по једно рјешење за сваку од конгруенција у посљедњем систему. Лако уочавамо да је $y_1 = y_2 = y_3 = 1$.

Сада формирамо рјешење почетног система конгруенција

$$x_0 = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 15 + 20 + 18 = 53$$

$$\begin{aligned} x &\equiv 53 \pmod{30} \\ x &\equiv 23 \pmod{30} \end{aligned}$$

Тако да сва рјешења задатог система конгруенција имају облик:

$$x = 23 + 30t\ ,\ t \in \mathbb{Z}$$

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`https://maths.ucd.ie/courses/math10040/Chapter3_13.pdf`

254

Користећи Ојлерову теорему ријешити конгруенцију:

$$36x \equiv 5 \pmod{49}$$

Доказ. Како је нзд$(36, 49) = 1$, можемо примијенити Ојлерову теорему:

$$\begin{aligned} \phi(49) &= \phi(7^2) \\ &= 7^2 - 7 \\ &= 42 \end{aligned}$$

По Ојлеровој теореми важи:

$$36^{42} \equiv 1 \pmod{49}$$

Помножимо ли задату конгруенцију са 36^{41} добијамо:

$$36x \equiv 5 \pmod{49} 36^{42}x \equiv 36^{41} \cdot 5 \pmod{49}$$

Како је $36^{42} \equiv 1 \pmod{49} \Rightarrow x \equiv 36^{41} \cdot 5 \pmod{49}$, па је сада је потребно одредити остатак при дијељењу 36^{41} бројем 49.

$$\begin{aligned} 36^{41} &\equiv (36^3)^{10} \cdot (36^3)^3 \cdot 36^2 \pmod{49} \\ &\equiv (85)^2 \cdot 8^3 \cdot 22 \pmod{49} \\ &\equiv 36^2 \cdot 22 \cdot 22 \pmod{49} \\ &\equiv 22 \cdot 22 \cdot 22 \pmod{49} \\ &\equiv 15 \pmod{49} \end{aligned}$$

Па је коначно рјешење конгруенције:

$$x \equiv 15 \cdot 5 \equiv 26 \pmod{49}$$

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
https://repozitorij.mathos.hr/islandora/object/mathos%3A260

255

Ријешити линеарну Диофантову једначину:

$$60x + 33y = 9$$

Доказ. Примијенимо Еуклидов алгоритам:

$$\begin{aligned} 60 &= 1 \cdot 33 + 27 \\ 33 &= 1 \cdot 27 + 6 \\ 27 &= 4 \cdot 6 + \underline{3} \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

Посљедњи ненулти остатак је број 3, па је $d = \text{нзд}(60, 33) = 3$. И како $3 \mid 9 \Rightarrow$ дата једначина има рјешење.
Како сваки остатак у алгоритму можемо приказати као линеарну комбинацију претходна два, то га можемо приказати и као линеарну комбинацију бројева a и b. Из тога специјално слиједи да и $\text{нзд}(a, b)$, можемо приказати као линеарну комбинацију бројева a и b.

$$\begin{aligned} 3 &= 27 - 4 \cdot 6 \\ &= 27 - 4 \cdot (33 - 27) \\ &= 5 \cdot 27 - 4 \cdot 33 \\ &= 5 \cdot (60 - 33) - 4 \cdot 33 \\ &= 5 \cdot 60 - 9 \cdot 33 \end{aligned}$$

Како је $\alpha = 5$ и $\beta = -9$ једно од рјешења једначине је:

$$x_0 = \alpha \cdot \frac{c}{d} = 5 \cdot \frac{9}{3} = 15$$
$$y_0 = \beta \cdot \frac{c}{d} = -9 \cdot \frac{9}{3} = -27$$

Скуп свих рјешења је облика:

$$\left\{ (x_0 + \frac{b}{d} \cdot t, y_0 - \frac{a}{d} \cdot t) \ / \ t \in \mathbb{Z} \right\}$$

Односно:

$$\left\{ (15 + 11t, -27 - 20t) \ / \ t \in \mathbb{Z} \right\}$$

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
https://www.diva-portal.org/smash/get/diva2:530204/FULLTEXT01.pdf

256

Ријешити линеарну Диофантову једначину:

$$57x + 22y = 400$$

Доказ. Примијенимо Еуклидов алгоритам:

$$\begin{aligned} 57 &= 22 \cdot 2 + 13 \\ 22 &= 13 \cdot 1 + 9 \\ 13 &= 9 \cdot 1 + 4 \\ 9 &= 4 \cdot 2 + \underline{1} \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

Посљедњи ненулти остатак је број 1, па је $d = \text{нзд}(57, 22) = 1$. И како $1 \mid 400 \Rightarrow$ дата једначина има рјешење.
Како сваки остатак у алгоритму можемо приказати као линеарну комбинацију претходна два, то га можемо приказати и као линеарну комбинацију бројева a и b. Из тога специјално слиједи да и $\text{нзд}(a, b)$, можемо приказати као линеарну комбинацију бројева a и b.

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 \\ &= 9 - 2 \cdot (13 - 9) \\ &= 3 \cdot 9 - 2 \cdot 13 \\ &= 3 \cdot (22 - 13) - 2 \cdot 13 \\ &= 3 \cdot 22 - 5 \cdot 13 \\ &= 3 \cdot 22 - 5 \cdot (57 - 2 \cdot 22) \\ &= -5 \cdot 57 + 13 \cdot 22 \end{aligned}$$

Како је $\alpha = -5$ и $\beta = 13$ једно од рјешења једначине је:

$$x_0 = \alpha \cdot \frac{c}{d} = -5 \cdot \frac{400}{1} = -2000$$
$$y_0 = \beta \cdot \frac{c}{d} = 13 \cdot \frac{400}{13} = 5200$$

Скуп свих рјешења је облика:

$$\left\{ (x_0 + \frac{b}{d} \cdot t, y_0 - \frac{a}{d} \cdot t) \ / \ t \in \mathbb{Z} \right\}$$

Односно:

$$\left\{ (-2000 + 22t, 5200 - 57t) \ / \ t \in \mathbb{Z} \right\}$$

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`https://www.diva-portal.org/smash/get/diva2:530204/FULLTEXT01.pdf`

257

Наћи све парове простих бројева p, q за које $pq \mid (5^p - 2^p)(5^q - 2^q)$

Доказ. Јасно је да су p и q непарни. Примијетимо да ако $p \mid (5^p - 2^p) \equiv 3 \pmod{p}$, онда је $p = 3$. Претпоставимо да је p = 3 (аналогно за q = 3). Тада је:

$$3q \mid (5^3 - 2^3)(5^q - 2^q) = 3^2 \cdot 13(5^q - 2^q)$$

Одакле је $q = 3$ или $q = 13$.
Претпоставимо сада да је $p > q > 3$. Тада $p \mid (5^q - 2^q)$ и $q \mid (5^q - 2^q)$. Како $q \mid (5^{q-1} - 2^{q-1})$, важи $5^n \equiv 2^n \pmod{q}$ за све n дјељиве са $q - 1$ или са p. При том су $q - 1$ и p узајамно прости, па постоје $x, y \in \mathbb{N}$ за које је $px = (q - 1)y + 1$. Тада је:

$$5 \cdot 2^{(q-1)y} \equiv 5 \cdot 5^{(q-1)y} \equiv 5^{px} \equiv 2^{px} = 2 \cdot 2^{(q-1)y} \pmod{q}$$

Одакле $q \mid 3 \cdot 2^{(q-1)y}$, што је контрадикција. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`https://imomath.com/srb/dodatne/stepene%20kongruencije_ddj.pdf`

258

Нека је n природан број и $F = 2^{2^n} + 1$. Доказати да је број F прост ако и само ако је $3^{\frac{F-1}{2}} \equiv -1 \pmod{F}$

Доказ. Претпоставимо да је:

$$3^{\frac{F-1}{2}} \equiv -1 \pmod{F}.$$

Нека је p неки прост дјелилац броја F. Како $p \mid 3^{F-1} - 1$, поредак броја 3 по модулу p дијели $F - 1 = 2^{2^n}$, дакле $\delta(3, p) = 2^k$ за неко k.
Ако је $k < 2^n$, онда $2^k \mid 2^{2^n-1} = \frac{F-1}{2}$ и према томе $3^{\frac{F-1}{2}} \equiv 1 \pmod{p}$ што није тачно. Слиједи да је $k = 2^n$, тј. $\delta(3, p) = 2^{2^n}$, одакле $2^{2^n} \mid p - 1$. То је могуће једино ако је $p = F$, тј. F је прост.

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`https://imomath.com/srb/dodatne/stepene%20kongruencije_ddj.pdf`

259

Нека је k дати природан број. Доказати да постоји бесконачно много потпуних квадрата облика $2^k n - 7$.

Доказ. Докажимо прво да за сваки природан број к постоји природан број a_k са особином

$$a_k^2 \equiv -7 \pmod{2^k}$$

Примијетимо да избор $a_k = 1$ задовољава тражени услов за $k \leq 3$.
За $k \geq 4$, пођимо од претпоставке $a_k^2 \equiv -7 \pmod{2^k}$. Сада је јасно да имамо двије могућности:

$$a_k^2 \equiv 2^k - 7 \pmod{2^{k+1}}$$

или

$$a_k^2 \equiv -7 \pmod{2^{k+1}}$$

У првом случају дефинишимо $a_{k+1} = a_k$, а у другом $a_{k+1} = a_k + 2^{k-1}$. Пошто је a_k непарно, слиједи:

$$a_{k+1}^2 = a_k^2 + 2^k a_k + 2^{2k-2} \equiv a_k^2 + 2^k a_k \equiv a_k^2 + 2^k \equiv -7 \pmod{2^{k+1}}$$

Најзад, примијетимо да низ a_k није ограничен, пошто мора бити $a_k^2 \geq 2^{k-1}$, што значи да посматрани низ има бесконачно много различитих вриједности. Отуда добијамо тражени резултат, пошто за $m \geq k$ имамо $a_m^2 \equiv -7 \pmod{2^k}$ и можемо дефинисати:

$$n = \frac{a_m^2 + 7}{2^k}$$

□

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`http://elibrary.matf.bg.ac.rs/handle/123456789/4790?show=full`

260

Доказати да за све природне бројеве m постоји природан број $n > m$ такав да се декадни запис броја 5^n добија дописивањем извјесног броја цифара слијева декадном запису броја 5^m.

Доказ. Услов задатка се може записати као

$$10^r \mid (5^n - 5^m)$$

гдје је r број цифара у декадном запису броја 5^m. Пошто је $r \leq m$, посматрана релација дјељивости је еквивалентна са $2^r \mid (5^n - 5^m) = 5^m(5^{n-m} - 1)$, тј. са

$$2^r \mid (5^{n-m} - 1),$$

Према Ојлеровој теореми, важи:

$$5^{\phi(2^r)} \equiv 1 \pmod{2^r}$$

Али, тада је очигледно да се за n облика:

$$n = m + \phi(2^r)k = m + 2^{r-1}k, \quad k \in \mathbb{N}$$

добија

$$5^n = 5^m(5^{\phi(2^r)})^k \equiv 5^m \pmod{2^r}$$

што се и тражило. □

(**Ирвин Хуремовић 19/17 Д**) задатак преузет из:
`http://elibrary.matf.bg.ac.rs/handle/123456789/4790?show=full`

261

Решити једначину $96x + 68y = 48$.

Доказ. Проверимо прво да ли дата једначина има решења. За то је потребно испитати да ли $NZD(96, 68) \mid 48$, па пронађимо прво $NZD(96, 68)$:

$$\begin{aligned} 96 &= 1 \cdot 68 + 28 \\ 68 &= 2 \cdot 28 + 12 \\ 28 &= 2 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 \end{aligned}$$

Дакле $NZD(96, 68) = 4$, како $4 \mid 48$ закључујемо да наша једначина има решења. Сада нам је потребно једно решење једначине $96x + 68y = 4$, које ћемо наћи уз помоћ Еуклидовог алгоритма:

$$\begin{aligned} 4 &= 28 - 2 \cdot 12 \\ 4 &= 28 - 2 \cdot (68 - 2 \cdot 28) \\ 4 &= 5 \cdot 28 - 2 \cdot 68 \\ 4 &= 5 \cdot (96 - 68) - 2 \cdot 68 \\ 4 &= 5 \cdot 96 + (-7) \cdot 68 \end{aligned}$$

Дакле једно решење једначине $NZD(96, 68) = 4$ је (5,-7). Како је $48 : 4 = 12$, помножимо последњу релацију са 12. Добијамо да је:

$$96 \cdot 60 + 68 \cdot (-84) = 48;$$

одакле имамо једно решење полазне једначине и то је (60,-84). Сада је само остало да запишемо општи облик решења ове једначине:

$$\begin{aligned} x &= 60 + \tfrac{68}{4}t, \\ y &= -84 - \tfrac{96}{4}t, \end{aligned}$$

односно

$$\begin{aligned} x &= 60 + 17t, \\ z &= -84 - 24t. \end{aligned}$$

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

262

Решити систем конгруенција $2x \equiv 3(\text{mod } 7)$
$4x \equiv 5(\text{mod } 11)$.

Доказ. Како је $2x \equiv 3(\text{mod } 7)$, тада $7 \mid (2x-3)$, тј. постоји $y \in Z$ тако да је $2x-3=7y$, тј. добијамо $2x-7y=3$. Очигледно је да је решење ове Диофантове једначине $(x_0, y_0) = (5, 1)$, а како решење (x_0, y_0) задовољава једначину тада важи $2x_0 - 7y_0 = 3$. Одузимањем ове две једнацине добијамо:

$$2(x-x_0) - 7(y-y_0) = 0,$$

тј.,

$$y - y_0 = \frac{2(x-x_0)}{7}.$$

Па важи:

$$\frac{x-x_0}{7} = t, t \in Z$$

одакле добијамо да је $x = 7t+5, t \in Z$. Уврстимо ли то решење у другу конгруенцију, добијамо:

$$\begin{gathered} 4(7t+5) \equiv 5(\text{mod } 11), \\ 28t + 20 \equiv 5 \ (\text{mod } 11) \\ 28t \equiv -15(\text{mod } 11) \\ 6t \equiv 7(\text{mod } 11). \end{gathered}$$

Решимо ли сада конгруенцију $6t \equiv 7(\text{mod } 11)$ добијамо да је њено решење $t \equiv 3 \ (\text{mod } 11)$, тј. $t = 11k+3, k \in Z$. Уврстимо ли то у формулу за x добијамо

$$x = 7(3+11k) + 5 = 26 + 77k, k \in Z$$

па је решење полазног система

$$x \equiv 26 \ (\text{mod } 77):$$

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

263

Ријешимо конгруенцију
$x^3 + 2x - 3 \equiv 0(\text{mod } 45)$.

Доказ. Како је $(9, 5) = 1$, дану конгруенцију можемо раставити на

$$x^3 + 2x - 3 \equiv 0(\text{mod } 5),\ x^3 + 2x - 3 \equiv 0(\text{mod } 9).$$

Конгруенцију $x^3 + 2x - 3 \equiv 0(\text{mod } 5)$ смо ријешили у једном од претходних примјера и њена рјешења су $x \equiv 1, 3 \pmod 5$. На аналоган нацин преостаје нам ријешити конгруенцију $x^3 + 2x - 3 \equiv 0(\text{mod } 9)$.Имамо:

$$\begin{gathered} x = 0 : x3 + 2x - 3 \equiv -3 \pmod 9 \\ x = 1 : x3 + 2x - 3 \equiv 0 \pmod 9 \\ x = 2 : x3 + 2x - 3 \equiv 0 \pmod 9 \\ x = 3 : x3 + 2x - 3 \equiv 3 \pmod 9 \\ x = 4 : x3 + 2x - 3 \equiv 6 \pmod 9 \\ x = 5 : x3 + 2x - 3 \equiv 6 \pmod 9 \\ x = 6 : x3 + 2x - 3 \equiv 0 \pmod 9 \end{gathered}$$

Дакле, рјешења су $x \equiv 1, 2, 6 \pmod 9$.
Сада комбинирањем претходних рјешења, имамо 6 система линеарних конгруенција који се рјешавају примјеном Кинеског теорема о остатцима.

$$\begin{gathered} 1.x \equiv 1 \pmod 5 \; x \equiv 1 \pmod 9 \Rightarrow x \equiv 1 \pmod{45}. \\ 1.x \equiv 1 \pmod 5 \; x \equiv 2 \pmod 9 \Rightarrow x \equiv 11 \pmod{45}. \\ 1.x \equiv 1 \pmod 5 \; x \equiv 6 \pmod 9 \Rightarrow x \equiv 6 \pmod{45}. \\ 1.x \equiv 3 \pmod 5 \; x \equiv 1 \pmod 9 \Rightarrow x \equiv 28 \pmod{45}. \\ 1.x \equiv 3 \pmod 5 \; x \equiv 2 \pmod 9 \Rightarrow x \equiv 38 \pmod{45}. \\ 1.x \equiv 3 \pmod 5 \; x \equiv 6 \pmod 9 \Rightarrow x \equiv 33 \pmod{45}. \end{gathered}$$

Стога су сва рјешења полазне конгруенције дана с $x \equiv 1, 6, 11, 28, 33, 38 \pmod 5$.

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
`https://repozitorij.mathos.hr/islandora/object/mathos%3A260/datastream/PDF/view`

264

Доказати да постоји к узастопних природних бројева од којих је сваки дељив са квадратом природног броја већег од 1.

Доказ. Нека су $p_1, p_2, \ldots, p_k$ различити прости бројеви. По Кинеској теореми о остацима систем

$$x \equiv -1(\text{mod } p_1^2),\ x \equiv -2(\text{mod } p_2^2), \ldots, x \equiv -k(\text{mod } p_k^2)$$

има решење. Ово значи да бројеви $x+1, x+2, \ldots, x+k$ имају тражену особину. Наиме $x+i$ је дељив са p_i^2 и за $i = 1, 2, \ldots, k$. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

265

Наћи све природне бројеве $m, n \geq 2$ такве да је $\frac{1+m^{3^n}+m^{2\cdot 3^n}}{n}$ цео број.

Доказ. Нека m и n задовоqавају услове задатка. Тада је н непаран број и $(m, n) = 1$. Ако је $n = 3$, тада је $m \equiv 1 \pmod 3$, јер би у слушају $m \equiv -1 \pmod 3$ имали

$$1 + m^{3^n} + m^{2\cdot 3^n} \equiv 1 - 1 + 1 \equiv 1 (\text{mod } 3)$$

Нека је сада $n > 3$. Тада важи $m^{3^n} \equiv 1 \pmod n$ јер би у супротном следило $1+m^{3^n}+m^{2\cdot 3^n} \equiv 1 - 1 + 1 \equiv 3 (\text{mod } n)$, тј. $n \mid 3$. Пошто је

$$1 + m^{3^n} + m^{2\cdot 3^n} = \frac{m^{3^{n+1}}-1}{m^{3^n}-1},$$

то је $m^{3^{n+1}} \equiv 1 (\text{mod } n)$. Нека је k најмањи природан број такав да је $m^k \equiv 1 (\text{mod } n)$. Тада $k \mid 3^{n+1}$ и $k \nmid 3^n$, па је $k = 3^{n+1}$. Како је $(m, n) = 1$ на основу Ојлерове теореме је $m^{\phi(n)} \equiv 1 \pmod n$, па је $k \leq \phi(n)$. Према томе, $3^{n+1} \leq \phi(n) \leq n - 1$, што је немогуће.
Дакле, тражени бројеви су $n = 3$ и сви бројеви $m \geq 4$ такви да је $m \equiv 1 \pmod 3$.

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

266

Доказати да за сваки природан број n важи $2^{4\cdot 5^{n-1}} \equiv 1 \pmod{5^n}$.

Доказ. Како је $\phi(5^n) = 4 \cdot 5^{n-1}$ и како су бројеви 2 и 5^n узајамно прости то је на основу Ојлерове теореме

$2^{\phi}(5n) = 2^{4\cdot 5n-1} \equiv 1 \pmod{5^n}$. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

267

Доказати да за све природне бројеве m постоји природан број $n > m$ такав да се декадни запис броја 5^n добија дописивањем извесног броја цифара слева декадном запису броја 5^m.

Доказ. Услов задатка се може записати као $10^r \mid (5^n - 5m)$, где је r број цифара у декадном запису броја 5^m. Пошто је $r \leq m$, посматрана релација дељивости је еквивалентна са $2^r \mid (5^n - 5m) = 5^m(5^{n-m} - 1)$, тј. са

$$2^r \mid (5^{n-m} - 1).$$

Према Ојлеровој теореми, важи:

$$5^{\phi(2^r)} \equiv \pmod{2^r}.$$

Али, тада је очито да се за n облика

$$n = m + \phi(2^r)k = m + 2^{r-1}k, k \in N.$$

добија што се и тражило

$$5^n = 5^m(5^{\phi(2r)})^k \equiv 5^m(mod 2^r).$$

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1

268

Наћи остатак при дељењу 3^{10^5} са 35.

Доказ. Како је (3,35)=1, на основу Ојлерове теореме, следи

$$3^{\phi(35)} \equiv 1 \pmod{35}$$
$$\phi(35) = \phi(7) \cdot 0\phi(5) = 6 \cdot 4 = 24$$
$$10^5 = 10000 = 24 \cdot 4166 + 16,$$

одавде следи

$$3^{10^5} \equiv (3^{24})^{4166} \cdot 3^16 \pmod{35}$$

Како је

$$3^{24} \equiv 1 \pmod{35} \Rightarrow 3^{10^5} \equiv 3^{16} \pmod{35}$$
$$3^4 \equiv 11 \pmod{35} \Rightarrow 3^{16} \equiv 11^4 \pmod{35}$$
$$11^2 \equiv 16 \pmod{35} \Rightarrow 11^4 \equiv 16^2 \pmod{35}$$
$$16^2 \equiv 11 \pmod{35}$$

Дакле, остатак је 11. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1

269

Ријеши линеарну диофантову једначину $27x + 59y = 20$:

Доказ. Она има решење, јер је $1 = NZD(27, 59)$, а 1 је делитељ броја 20. Овде је $a = 58, b = 27$, користећи Еуклидов алгоритам добијамо

$$59 = 2 \cdot 27 + 5$$
$$27 = 5 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1.$$

Бројеви 27 и 59 су узајамно прости, па број 1 можемо представити као линеарну функцију борјева 27 и 59.

$$1 = 5 - 2 \cdot 2 = 5 - 2(27 - 5 \cdot 5) = 11 \cdot 5 - 2 \cdot 27$$
$$= 11(59 - 2 \cdot 27) - 2 \cdot 27 = 11 \cdot 59 - 24 \cdot 27.$$

Коначно добијамо да је $(-480)27 + 220 \cdot 59 = 20$.

Дакле, једно решење линеарне Диофантове једначине $27x + 59y = 20$ је (-480, 220). Лако се проверава да су решења и $x = -480 + 59t, y = 220 - 27t$, где је t цео број. Може се изабрати И мање (по апсолутној вредности) почетно решење. На пример, за t= 8 се добија $x_1 = -8, y_1 = 4$, па је опште решење $x = -8 + 59u, y = 4 - 27u, u \in Z$. □

(**Данијела Матановић 38/18 Д**) задатак преузет са
https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic
pdf

270

Одредите последње три цифре броја $2^{2015} - 2^{2013} + 2^{2010}$.

Доказ. Потребно је одредити $x \in Z$ тако да је $0 \leq x < 1000$ и

$$2^{2015} - 2^{2013} + 2^{2010} \equiv k \pmod{1000}.$$

Имајмо на уму да за моћи броја 2 и модула $m = 1000$ не можемо применити Еулерову теорему јер је $NZD(2, 1000) = 2 > 1$. Али $1000 = 2^3 \cdot 5^3$, па применимо на $n = 125$.

$$2^{2015} - 2^{2013} + 2^{2010} = 2^{2000}(2^{15} - 2^{13} + 2^{10}) \equiv 2^{15} - 2^{13} + 2^{10} \equiv 100 \pmod{125}$$

од $2^{100} \equiv 1 \pmod{125}$ према теорему ,од $2^3 \mid 2^{2015}$ слиједи $2^{2013} + 2^{2010}$ да x задовољава следећи систем конгруенција

$$x \equiv 0 \pmod{8}, x \equiv 100$$

Према кинеском преосталом теорему, систем има јединствено решење модуло 1000.
Сва решења друге конгруенце $x \equiv 100 \pmod{125}$ за $0 \leq x < 1000$ су

$$100, 225, 350, 475, 600, 725, 850, 975.$$

Међу њима је једино 600 дјељив с 8 па је $x = 600$.

□

(**Данијела Матановић 38/18 Д**) задатак преузет са
https://repozitorij.mathos.hr/islandora/object/mathos%3A260/datastream/PDF/view

271

Желимо да направимо RSA криптограгију са $n = pq$ гдје је $p = 11$ и $q = 13$:

а) Која је најмања могућа вриједност декодираног експонента e коју можемо узети

б) Узмимо e да буде једнако тој вриједности, наћи декодирани експонент d

в) Боб жели да каже Алиси којег дана у мају је рок за израду збирке из криптографије. Какву поруку ће он послати Алиси?

Доказ. а) Имамо $\Phi(n) = 10 \cdot 12 = 120$. Треба да нађемо e да буде веће од 1 и релативно просто у односу на $\Phi(n)$, то значи да је најмања могућа вриједност $e - 7$.

б) Цијели број d мора бити инверзан $e = 7 \pmod{120}$ Примјетимо да
$7 \cdot 17 = 119 \equiv -1 \pmod{120}$
дакле $7 \cdot 103 \equiv 7 \cdot (-17) \equiv 1 \pmod{120}$, па нам $d = 103$ сасвим одговара

в) Жеимо да пошаљемо број 29 За тај број израчунавање би било
$20^2 = 841 \equiv 126 \equiv -17 \pmod{143}$
у следећем кораку квадрирамо све, $29^4 \equiv (-17)^2 \equiv 3 \pmod{143}$
Слиједи $29^7 = 29^4 \cdot 29^2 \cdot 29 \equiv 3 \cdot (-17) \cdot 29 = -1479 \equiv -49 \equiv \pmod{143}$.
Дакле Боб ће послати број 94 Алиси.

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://cims.nyu.edu/~bilu/NT%20homework%207%20solution.pdf`

272

Два играча играју следећу игру: први играч записује једну цифру; затим други играч дописује са леве или десне стране неку цифру; затим први дописује са леве или десне стране неку цифру; затим други поново дописује са леве или десне стране неку цифру итд. Показати да први играч може играти тако да после сваког потеза другог играча записани број није потпуни квадрат.

Доказ. Прва цифра коју први играч треба да запише мора бити 7 јер је то једина цифра таква да не постоји двоцифрен квадрат који почиње или завршава се са 7. Затим претпоставимо да је у неком тренутку, након потеза другог играча, записан број $c_1c_2c_3 \dots c_{2k-1}c_{2k}$. Први играч сада треба да допише 7 или 8 са десне стране. У том случају, уколико други играч допише било коју цифру са леве стране, добијени број неће бити потпун квадрат јер се ниједан потпун квадрат не завршава цифрама 7 или 8. Уколико други играч допише

било коју цифру са десне стране, добиће се један одследећих бројева:

$$c_1c_2c_3\ldots c_{2k-1}c_{2k}70, c_1c_2c_3\ldots c_{2k-1}c_{2k}71, \ldots, c_1c_2c_3\ldots c_{2k-1}c_{2k}89.$$

Ради се о 20 узастопних бројева већих од 1000 па међу њима не могу бити два која су потпуни квадрати. У случају да међу њима нема ниједан потпун квадрат, први играч може да допише било коју од цифара 7 или 8. Ако је један од уочених бројева потпун квадрат и ако је његова претпоследња цифра 7, први играч треба да допише 8 а у супротном случају цифру 7. У било ком од претпостављених случајева други играч не може формирати потпун квадрат дописивањем било које од цифара. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

273

Показати да је $a^{25} - a$ дјељив са 30 за сваки цијели број a.

Доказ. То ћемо показати тако што ћемо потврдити дјељивост датог израза са 5, 3 и 2. Најприје, имамо на основу Теореме М.Ф. да је $a^5 \equiv a \pmod 5$, па је

$$a^{25} \equiv (a^5)^5 \equiv a^5 \equiv a \pmod 5,$$

одакле је $5 \mid a^{25} - a$. Слично, из $a^3 \equiv a \pmod 3$ имамо

$$a^{25} \equiv (a^3)^8 a \equiv a^8 a \equiv a^9 \equiv (a^3)^3 \equiv a^3 \equiv a \pmod 3.$$

Закључујемо да је $3 \mid a^{25} - a$. На крају, из $a^2 \equiv a \pmod 2$, слиједи

$$a^{25} \equiv (a^2)^{12} a \equiv a^{12} a \equiv \ldots \equiv a^3 a \equiv (a^2)^2 \equiv a^2 \equiv a \pmod 2,$$

што повлачи $2 \mid a^{25} - a$. Како је израз $a^{25} - a$ дјељив са 2, 3 и 5, онда је дјељив са 30 за сваки цијели број a. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

274

Доказати да за произвољно $\epsilon > 0$ постоји природан број n тако да

$$\frac{\phi(n)}{n} > 1 - \epsilon.$$

Доказ. Пошто је скуп простих бројева бесконачан, онда за свако $\epsilon > 0$ постоји прост број p тако да $p > 1/\epsilon$. За $n = p^e$, гдје је $e \in \mathbb{N}$, имамо да

$$\frac{\phi(n)}{n} = 1 - \frac{1}{p} > 1 - \epsilon.$$

□

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

275

Одредимо све природне бројеве n за које вриједи $\phi(n) = 12$.

Доказ. Нека је дата факторизација $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Слиједи

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1).$$

Пошто фактори облика $p_i - 1$ дијеле $\phi(n)$, онда слиједи да $(p_i - 1) \mid 12$. Закључујемо да $p_i \in \{2, 3, 5, 7, 13\}$, те да $5, 7, 13$ могу у факторизацији броја n могу имати највише степен 1, док 2 може имати највише до трећег, а 3 до највише другог степена. Дакле,

$$n = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} 7^{\alpha_4} 13^{\alpha_5},$$

$\alpha_1 \leq 3, \alpha_2 \leq 2$, док $\alpha_3, \alpha_4, \alpha_5 \leq 1$. Такође, лако се уочава да највише један од експонената $\alpha_3, \alpha_4, \alpha_5$ може бити јединица. Значи, имамо укупно четири могућности $n = 2^{\alpha_1} 3^{\alpha_2}$, $n = 5 \cdot 2^{\alpha_1} 3^{\alpha_2}$, $n = 7 \cdot 2^{\alpha_1} 3^{\alpha_2}$, $n = 13 \cdot 2^{\alpha_1} 3^{\alpha_2}$. Рецимо да је $n = 7 \cdot 2^{\alpha_1} 3^{\alpha_2}$. Онда је $\phi(n) = 6 \cdot \phi(k)$, гдје је $k = 2^{\alpha_1} 3^{\alpha_2}$. Слиједи да је $\phi(k) = 2$, одакле је $k \in \{3, 4, 6\}$, па је у овом случају $n \in \{21, 28, 42\}$. Директном провјером за сваку од наведених могућности, добијамо $n \in \{13, 21, 26, 28, 36, 42\}$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

276

Наћи:

а) $\phi(529)$

б) $\phi(29791)$

в) $\phi(400)$

Доказ. а) Примјетимо како је $529 = 23^2$. Пошто је 23 прост број имамо:
$\phi(529) = \phi(23^2) = 23^2 - 23 = 506$

б) Примјетимо да је $29791 = 31^3$. Пошто је 31 прост број имамо:

$\phi(29791) = \phi(31^3) - (31^2) = 29791 - 961 = 28830$

в) Када 400 разложимо на просте чиниоце имамо $400 = 2^4 \cdot 5^2$ дакле:

$$\phi(400) = \phi(2^4 \cdot 5^2 = \phi(2^4)\phi(5^2) = (2^4 - 2^3)(5^2 - 5^1) = (8)(24) = 160$$

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`http://mathonline.wikidot.com/euler-s-totient-function-examples-1`

277

Нека је број $2^k + 1$ прост. Доказати да је тада $k = 0$ или $k = 2^n$ за неки $n \geq 0$.

Доказ. Претпоставимо да k има неки непаран прости фактор p. Тада из $k = p \cdot m$ слиједи да је број

$$2^k + 1 = (2^m)^p + 1^p = (2^m + 1)(2^{m(p-1)} - 2^{m(p-2)} + \cdots + 1)$$

дељив с $2^m + 1$, па није прост.
Бројеви $f_n = 2^{2^n} + 1$ називају се Фермаови бројеви. Фермао је сматрао да су сви они прости. Заиста, $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$ и $f_4 = 65537$ су прости. Међутим, $f_5 = 2^{32} + 1$ је сложен. Покажимо то!

$$\begin{aligned} 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = (641 - 5^4) \cdot 2^{28} + 1 &= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 \\ &= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641 \cdot (2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4) \end{aligned}$$

Према томе, $641 \mid f_5$.
Закључак је да је само коначно много Фермаових бројева просто. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

278

Доказати да не постоји полином $f(x)$ с цјелобројним коефицијентима, степена ≥ 1, такав да је $f(n)$ прост за све $n \in \mathbb{N}$.

Доказ. Нека је $f(1) = p$. Тада је p прост број. Будући да је $f(1 + kp) - f(1)$ дељиво са $(1 + kp) - 1 = kp$ (јер $x - y$ дијели $x^m - y^m$), слиједи да $p \mid f(1 + kp)$, за сваки $k \in N$. Међутим, $f(1 + kp)$ је прост, па мора бити $f(1 + kp) = p, \forall k \in \mathbb{N}$. Будући да полином $f(x) - p$ има бесконачно много нултачака, он мора бити нулполином, па је $f(x) = p$, што је у супротности с претпоставком да је ст $f \geq 1$.
Пуно тежи проблем је одредити полиноме $f(x)$ такве да је $f(n)$ прост за бесконачно много природних бројева n. Зна се да то вриједи за линеарне полиноме $f(x) = ax + b$ ако је $(a, b) = 1$. Но, већ за полином $f(x) = x^2 + 1$, то је отворено питање. Закључак је да тврдња вриједи за све полиноме који су иредуцибилни и за које не постоји природан број $d > 1$ такав да $d \mid f(n)$, $\forall n \in \mathbb{N}$. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

279

Нека је n природан број. Доказати да је број

$$(n+1)(n+2)\cdots(n+n)$$

дељив са 2^n, а није дељив са 2^{n+1}.

Доказ. Доказаћемо индукцијом да се број 2 појављује тачно n пута као чинилац броја $(n+1)(n+2)\cdots(n+n)$.
За $n=1$ тврђење је очигледно тачно, јер је тада дати производ једнак 2.
Претпоставимо да се, за неки природан број n, број 2 у производу $(n+1)(n+2)\cdots(n+n)$ појављује као чинилац тачно n пута. Тада је
$(n+1+1)(n+1+2)\cdots(n+1+n-1)(n+1+n)(n+1+n+1)$
$=(n+2)(n+3)\cdots(n+n)(2n+1)(2n+2)$
$=(n+2)(n+3)\cdots(n+n)(2n+1)2(n+1)$
$=2(n+1)(n+2)(n+3)\cdots(n+n)(2n+1)$
па пошто се, према индукцијској претпоставци, 2 појављује тачно n пута као чинилац у производу $(n+1)(n+2)\cdots(n+n)$, а чинилац $2n+1$ је непаран те он није дељив са 2, следи да се у производу $(n+1+1)(n+1+1)\cdots(n+1+n-1)(n+1+n)(n+1+n+1)$ број 2 као чинилац појављује тачно $n+1$ пута. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

280

Ријешити систем конгруенција

$$x\equiv 3 \pmod{10},\quad x\equiv 8 \pmod{15},\quad x\equiv 5 \pmod{84}.$$

Доказ. Уочимо да бројеви 10, 15 и 84 нису у паровима релативно прости, па не можемо Кинеску теорему о остацима примјенити директно, а може се догодити да такав систем уопште нема рјешења. Сада поступамо овако. Наш систем је еквивалентан са

$$x\equiv 3 \pmod{2},\quad x\equiv 3 \pmod{5},\quad x\equiv 8 \pmod{3},\quad x\equiv 8 \pmod{5},$$
$$x\equiv 5 \pmod{4},\quad x\equiv 5 \pmod{3},\quad x\equiv 5 \pmod{7}$$

Дакле, модули су нам потенције простих бројева и сада упоредимо конгруенције које одго-

варају истом простом броју:

$$\begin{aligned} x \equiv 3 \pmod 2, \quad x \equiv 5 \pmod 4 &\iff x \equiv 1 \pmod 4 \\ x \equiv 8 \pmod 3, \quad x \equiv 5 \pmod 3 &\iff x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5, \quad x \equiv 8 \pmod 5 &\iff x \equiv 3 \pmod 5 \\ & \quad x \equiv 5 \pmod 7. \end{aligned}$$

□

Дакле, наш систем је еквивалентан систему

$$x \equiv 1 \pmod 4, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 5 \pmod 7$$

на који можемо примијенити Кинеску теорему о остацима.Имамо:
$m = 4 \cdot 3 \cdot 5 \cdot 7 = 420, n_1 = 105,\ n_2 = 140,\ n_3 = 84,\ n_4 = 60,$

$$\begin{aligned} 105x_1 \equiv 1 \pmod 4 &\iff x_1 \equiv 1 \pmod 4 \Rightarrow x_1 = 1, \\ 140x_2 \equiv 2 \pmod 3 &\iff 2x_2 \equiv 2 \pmod 3 \Rightarrow x_2 = 1, \\ 84x_3 \equiv 3 \pmod 5 &\iff 4x_3 \equiv 3 \pmod 5 \Rightarrow x_3 = 2, \\ 60x_4 \equiv 5 \pmod 7 &\iff 4x_4 \equiv 4 \pmod 7 \Rightarrow x_4 = 3. \end{aligned}$$

Дакле, рјешење је

$$x \equiv 105 \cdot 1 + 140 \cdot 1 + 84 \cdot 2 + 60 \cdot 3 = 593 = 173 \pmod{420}.$$

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

281

Одредити све тројке $(p, q, r)(q \leq r)$ простих бројева за које важи $p^2 + qr = 1996^2$.

Доказ. Дату једнакост можемо записати и овако:

$$qr = 1996^2 - p^2 = (1996 - p)(1996 + p).$$

Разликујемо три случаја:
1. $p = 3$: из $qr = 1993 \cdot 1999$ слиједи $q = 1993$ и $r = 1999$;
2. $p = 3k + 1$: тада $3 \mid 1996$ - p па мора бити $q = 3$. Из $r = (665 - k)(1996 + p$ слиједи $665 - k = 1$, па је $p = 1993$ и $r = 3989$;
3. $p = 3k + 2$: тада $3 \mid 1996 + p$ па је опет $q = 3$. Из $r = (1996 - p)(666 + k)$, како је $p \geq 2$, добијамо да је r сложен број, па овај случај не даје рјешење. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

282

Доказати да постоји бесконачно много природних бројева n таквих да једначина $(x+y+z)^3 = n^2xyz$ има рјешење у скупу природних бројева.

Доказ. Потражимо рјешења x, y, z дате једначине таква да је $z = k(x+y)$, где је k природан број. Тада дату једначину можемо записати у облику:

$$((x+y)+k(x+y))^3 = n^2xyk(x+y)$$

тј.(*)

$$(k+1)^3(x+y)^2 = n^2kxy.$$

Ако једначина (*) има рјешење за неке n и k онда је то случај и са задатом једначином. Нека је $n = 3k+3$. Тада се (*) може записати у облику

$$(k+1)(x+y)^2 = 9kxy.$$

Довољно је доказати да последња једначина има рјешewe (x, y) за бесконачно много k, или еквивалентно, да квадратна једначина по t $t = \frac{x}{y}$

$$(k+1)(t+1)^2 - 9kt = 0, \text{ тј. } (k+1)t^2 - (7k-2)t + (k+1) = 0$$

има позитивно рационално рјешење за бесконачно много к. Последње тврђење важи ако и само ако је дискриминанта

$$D = (7k-2)^2 - 4(k+1)^2 = 9k(5k-4)$$

потпун квадрат за бесконачно много k. Стављајући да је $k = u^2$ проблем се своди на доказивање да једначина

$$5u^2 - 4 = v^2$$

има бесконачно много рјешења (u, v) у скупу цијелих бројева.

□

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

283

Ако је D природан број облика $4k+3$, $k \in N$, доказати да једначина $x^2 - Dy^2 = -1$ нема рјешења у скупу природних бројева.

Доказ. Квадрати природних бројева при дијељењу са 4 могу давати остатак 0 или 1. Дакле, ако би дата једначина имала рјешења (x, y), имали бисмо да је

$$Dy^2 \equiv 0 \pmod 4 \text{ или } Dy^2 \equiv 3 \pmod 4,$$

док је

$$x^2 + 1 \equiv 1 \pmod 4 \text{ или } x^2 + 2 \equiv 2 \pmod 4$$

□

(**Јована Шубарић 11/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

284

Доказати да за сваки природан број $n > 1$ не постоји строго растући низ природних бројева $a_1, a_2, \ldots, a_n$ такав да је

$$\frac{1}{a_1^2} + \frac{1}{a_2^2} + \ldots + \frac{1}{a_n^2} = 1$$

Доказ. Сигурно је $a_1 \neq 1$, па из $a_1 < a_2 < \cdots < a_n$ слиједи да је $a_1 \geq 2, a_2 \geq 3, \ldots, a_n \geq n+1$, па је

$$\frac{1}{a_1^2} \leq \frac{1}{2^2}, \frac{1}{a_2^2} \leq \frac{1}{3^2}, \ldots, \frac{1}{a_n^2} \leq \frac{1}{(n+1)^2}.$$

Сада је
$\frac{1}{a_1^2} + \frac{1}{a_2^2} + \cdots + \frac{1}{a_n^2} \leq \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(n+1)^2} \leq \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \cdots + \frac{1}{n} - \frac{1}{n+1} = 1 - \frac{1}{n} < 1,$
па једначина нема рјешења. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf

285

Наћи све природне бројеве n такве да једначина

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} = \frac{n+1}{x_{n+1}^2}$$

има рјешење у скупу природних бројева.

Доказ. Ако је $n = 1$, једначина постаје $2 = \frac{x_2^2}{x_1^2}$ и, пошто је $\sqrt{2}$ ирационалан број, једначина нема рјешења у скупу природних бројева.
Ако је $n = 2$ имамо

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} = \frac{3}{x_3^2},$$

односно $(x_2x_3)^2 + (x_1x_3)^2 = 3(x_1x_2)^2$, тј. $a^2 + b^2 = 3c^2$ за $a = x_2x_3, b = x_1x_3$ и $c = x_1x_2$.Пошто су квадрати циелих бројева конгруентни 0 или 1 по модулу 3, закључујемо да су a и b дјељиви са 3. Нека је $a = 3a_1$ и $b = 3b_1$. После замјене и скраћивања закључујемо да је и c дјељиво са 3. Нека је $c = 3c_1$. Онда добијамо $a_1^2 + b_1^2 = 3c_1^2$.На исти начин се показује да су a_1, b_1 и c_1 дјељиви са 3 итд. Према томе, за свако $m \in N$ су бројеви a, b и c дјељиви са 3^m, што је могуће само ако је $a = b = c = 0$. Контрадикција, јер је $a = x_2x_3 \neq 0$.
Покажимо сада да за $n \geq 3$ дата једначина има рјешења у скупу N. Довољно је доказати да то важи за $n = 3$. Наиме, ако је

$$\frac{1}{x_1^2}+\frac{1}{x_2^2}+\frac{1}{x_3^2}=\frac{4}{x_4^2}$$

тада је

$$\frac{1}{x_1^2}+\frac{1}{x_2^2}+\frac{1}{x_3^2}+\frac{1}{x_4^2}+\cdots+\frac{1}{x_4^2}=\frac{n+1}{x_4^2}.$$

Да бисмо нашли рјешење за $n=3$, уочимо једнакост

$$\frac{1}{15^2}+\frac{1}{20^2}=\frac{1}{12^2}.$$

Сада је

$$\frac{1}{15^2}\cdot\frac{1}{12^2}+\frac{1}{20^2}\cdot\frac{1}{12^2}=\frac{1}{(12^2)^2},$$

одакле добијамо

$$\frac{1}{(15\cdot 12)^2}+\frac{1}{(20\cdot 15)^2}+\frac{1}{(20\cdot 20)^2}=\frac{1}{(12^2)^2}=\frac{4}{(2\cdot 12^2)^2}.$$

□

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

286

Neka su m i n prirodni brojevi takvi da

$$m \mid n^2,\ n^2 \mid m^3,\ m^3 \mid n^4,\ n^4 \mid m^5,\ \ldots$$

Доказати да је $m=n$.

Доказ. Нека је:

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_l^{\alpha_l},\ n=p_1^{\beta_1}p_2^{\beta_2}\cdots p_l^{\beta_l}$$

(неки од бројева α и β могу бити и једнаки нули). Из услова задатка добијамо да за свако $i\in\{1,2,\ldots,l\}$ важи:

$$\alpha_i\le 2\beta_i\le 3\alpha_i\le 4\beta_i\le 5\alpha_i\le 6\beta_i\le\ldots$$

одакле следи да је:

$$\alpha_i\le 2\beta_i,\ \beta_i\le\tfrac{3}{2}\alpha_i,\ \alpha_i\le\tfrac{4}{3}\beta_i,\ \beta_i\le\tfrac{5}{4}\alpha_i,\ \alpha_i\le\tfrac{6}{5}\beta_i,\ \beta_i\le\tfrac{7}{6}\alpha_i,\ \ldots,$$

тј.

$$\alpha_i\le\tfrac{2k}{2k-1}\beta_i\to\beta_i(k\to+\infty\text{ и }\beta_i\le\tfrac{2k+1}{2k}\alpha_i\to\alpha_i(k\to+\infty$$

па се добија $\alpha_i\le\beta_i$ и $\beta_i\le\alpha_i$, тј. $\alpha_i=\beta_i$ □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

287

Одредити сва рјешења једначине $4x+5y = 100$ ако су x и y цијели бројеви.

Доказ. Овде користимо метод почетног рјешења. Идеја је да нађемо једно очигледно рјешење а онда на основу тога и остала рјешења. Прво очигледно рјешење ове једначине је за $x_0 = 0$, $y_0 = 20$.
Теорема: Ако је уређени пар (x_0, y_0) једно рјешење линеарне Диофантове једначине $a+b = c$ и ($ab \neq 0$ и a и b су узајамно прости цијели бројеви) тада и само тада је релацијама $x = x_0 + nk$ и $y = y_0 - ak (k \in Z)$ дефинисано опште рјешење дате једначине.
Ако примјенимо ову теорему на нашу једначину добијамо:

$$x = 5k \text{ и } y = 20 - 4k.$$

Рјешење за y можемо добити и ако умјесто x у почетну једначину ставимо $x = 5k$:

$$4 \cdot 5k + 5y = 100$$

$$20k + 5y = 100$$

подјелимо лијеву и десну страну једначине са 5

$$4k + y = 20$$

$$y = 20 - 4k$$

Рјешење ове једначине је уређени пар $(x, y) = (5k, 20 - 4k)$, $k \in Z$. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

288

Ријешити систем конгруенција
$x \equiv 6 \pmod{11}$
$x \equiv 13 \pmod{16}$
$x \equiv 9 \pmod{21}$
$x \equiv 19 \pmod{25}$

Доказ. Пошто су $11, 16, 21$ и 25 међусобно релативно прости, Кинеска теорема о остацима нам говори да постоји јединствено ријешење по модулу m, гдје је $m = 11 \cdot 16 \cdot 21 \cdot 25 = 92400$
Употребимо Кинеску теорему о остацима са

$$k = 4$$
$$m_1 = 11, m_2 = 16, m_3 = 21, m_4 = 25$$
$$a_1 = 11, a_2 = 16, a_3 = 21, a_4 = 25$$

да би смо добили ријешење Имамо следећи поступак

$$\begin{aligned} z_1 &= m/m_1 = m_2m_3m_4 = 16 \cdot 21 \cdot 25 = 8400 \\ z_2 &= m/m_2 = m_1m_3m_4 = 11 \cdot 21 \cdot 25 = 5775 \\ z_3 &= m/m_3 = m_1m_2m_4 = 11 \cdot 16 \cdot 25 = 4400 \\ z_4 &= m/m_4 = m_1m_3m_3 = 11 \cdot 16 \cdot 21 = 3696 \end{aligned}$$

$$\begin{aligned} y_1 &\equiv {z_1}^{-1} \pmod{m_1} \equiv 8400^{-1} \pmod{11} \equiv 7^{-1} \pmod{11} \equiv 8 \pmod{11} \\ y_2 &\equiv {z_3}^{-1} \pmod{m_1} \equiv 5775^{-1} \pmod{16} \equiv 7^{-1} \pmod{16} \equiv 8 \pmod{16} \\ y_3 &\equiv {z_3}^{-1} \pmod{m_1} \equiv 4400^{-1} \pmod{21} \equiv 7^{-1} \pmod{21} \equiv 8 \pmod{21} \\ y_4 &\equiv {z_4}^{-1} \pmod{m_1} \equiv 3696^{-1} \pmod{25} \equiv 7^{-1} \pmod{25} \equiv 8 \pmod{25} \end{aligned}$$

$$\begin{aligned} w_1 &\equiv y_1z_1 \pmod{m} \equiv 8 \cdot 8400 \pmod{92400} \equiv 67200 \pmod{92400} \\ w_2 &\equiv y_2z_2 \pmod{m} \equiv 15 \cdot 5775 \pmod{92400} \equiv 86625 \pmod{92400} \\ w_3 &\equiv y_3z_3 \pmod{m} \equiv 2 \cdot 4400 \pmod{92400} \equiv 8800 \pmod{92400} \\ w_4 &\equiv y_4z_4 \pmod{m} \equiv 6 \cdot 3696 \pmod{92400} \equiv 22176 \pmod{92400} \end{aligned}$$

Ријешење чији је јединсвени модуо 92400 је

$$\begin{aligned} x &\equiv a_1w_1 + a_2w_2 + a_3w_3 + a_4w_4 \pmod{92400} \\ &\equiv 6 \cdot 67200 + 13 \cdot 86625 + 9 \cdot 8800 + 19 \cdot 22176 \pmod{92400} \\ &\equiv 2029849 \pmod{92400} \\ &\equiv 51669 \pmod{92400} \end{aligned}$$

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`http://homepages.math.uic.edu/~leon/mcs425-s08/handouts/chinese_remainder.pdf`

289

Нека је $d = \text{нзд}(a, b)$. Претпоставимо да је (x_0, y_0) решење једначине. Доказати да је тада

$$ax_0 + by_0 = c.$$

Доказ. Како $d \mid a$ и $d \mid b$, онда $d \mid c$.
Обратно, претпоставимо да $d \mid c$. Тада постоји цео број k такав да је $c = dk$. С друге стране d се може представити као линеарна функција од a и b, тј. постоје цели бројеви x' и y' такви да је

$$ax' + by' = d.$$

Множећи последњу једнакост са k, добијамо

$$akx' + bky' = dk.$$

тј.

$$a(kx') + b(ky') = c.$$

Дакле, добијено је једно решење $(x_0, y_0) = (kx', ky')$ Диофантове једначине $ax + by = c$

□

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

290

Конгруенција $P(x) \equiv 0(\mod p$ реда $n, n > p$, гдје је p прост број еквивалентна је конгруенцији $R(x)$ са $x^p - x$. Доказати.

Доказ. Нека је $Q(x)$ полином такав да је :

$$P(x) = (x^p - x)Q(x) + R(x)$$

Онда је дата конгруенција еквивалентна конгруенцији

$$(x^p - x)Q(x) + R(x) \equiv 0(\mod p)$$

Што на основу Мале Фермаове теореме такође еквивалентно конгруенцији

$$R(x) \equiv 0(\mod p)$$

Напомена, мала Фермаова теорема тврди да ако је p прост број, онда ће за сваки цијели број a, $(a^p - a)$ бити дјељиво са p □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

291

Ријешити конгруенцију

$$36x \equiv 5 \pmod{49}$$

Доказ. Како је $(36, 49) = 1$, можемо примјенити Ојлерову теорему. Па слиједи

$$\varphi(49) = \varphi(7^2) = 7^2 - 7 = 42.$$

Ојлерова теорема нам каже да вриједи

$$36^{42} \equiv 1 \pmod{49}.$$

Ако помножимо $36x \equiv 5 \pmod{49}$ са 36^{41} добијамо

$$36^{42}x \equiv 36^{41} \cdot 5 \pmod{49}.$$

Како је $36^{42} \equiv 1 \pmod{49}$ вриједи $x \equiv 36_{41} \cdot 5 \pmod{49}$. Сада је потребно одредити остатак при дијељењу 36^41 бројем 49.
$36^{41} \equiv (36^3)^{10} \cdot (36^3)^3 \cdot 36^2 \pmod{49}$
$36^{41} \equiv (8^5)^2 \cdot 8^3 \cdot 22 \pmod{49}$
$36^{41} \equiv 36^2 \cdot 22 \cdot 22 \pmod{49}$
$36^{41} \equiv 22 \cdot 22 \cdot 22 \pmod{49}$
$36^{41} \equiv 15 \pmod{49}$
према томе $x \equiv 15 \cdot 5 \equiv 26 \pmod{49}$

□

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

292

Доказати да једначина $2x + 5y = 111$ има бесконачно много цјелобројних рјешења , а једначина $3x + 6y = 1000$ нема цјелобројних рјешења.

Доказ. За рјешавање овог задатка користићемо теорему о линеарној Диофантовој једначини :
$ax + by = c$, гдје су a,b и c цијели бројеви и $ab \neq 0$

Једначина има увјек рјешење ако је НЗД$(a, b) = 1$, ако су a и b узајамно прости цијели бројеви .
Како су 2 и 5 узајамно прости прва једначина на основу горе наведене теореме увјек има рјешење .
Док друга једначина дјељењем са 3 се може записати у облику $x + 2y = \frac{1000}{3}$ из чега је очигледно да нема цјелобројних рјешења . □

(**Милош Ћупић 39/18 Д**) задатак преузет са

293

Ријешити линеарну конгруенцију

$$39x \equiv 6287 \pmod{826}$$

Доказ. Примјеном Еуклидовог алгоритма слиједи:

$$826 = 39 \cdot 21 + 7$$

$$39 = 7 \cdot 5 + 4$$

$$7 = 4 \cdot 1 + 3$$

$$3 = 1 \cdot 3$$

Дакле, $(39, 826) = 1$ и $1 \mid 6287$, па слиједи да постоји 1 рјешење полазне конгруенције. Према Еуклидовом алгоритму постоје u и v такви да $39u + 826v = 1$, тј. $39u \equiv 1 \pmod{826}$. Примјеном рекурзивних формула $u_{-1} = 0$, $u_0 = 1$, $u_i = u_{i-2} - u_{i-1} \cdot q_i$ слиједи нам таблица

i	-1	0	1	2	3	4
q_i	-	-	21	5	1	1
u_i	0	1	-21	106	-127	233

Дакле, $u \equiv 233 \pmod{826}$ је рјешење конгруенције. Сада имамо $39(6287u) \equiv 6287 \pmod{826}$, па је $6287u$ рјешење конгруенције. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

294

Два играча играју следећу игру.Први изговори било који природан број, други додаје том броју 54 или 77, и изговара добијени збир. У наставку играчи наизмјенично додају било који од бројева 54 и 77 и изговарају збир тог броја са претходним збиром. Други играч постиже побједу ако било који од играча изговори број чији остатак при дијељењу са 100 прост број. Може ли први да онемогући другом играчу побједу ?

Доказ. Не. Наиме, стратегија другог играча је следећа:
Нека први на почетку изабере број n. Други бира рецимо 54. Затим у сваком следећем потезу бира број који први играч није бирао у истом потезу.
Тако се након k-тог потеза добија број

$$n + 54 + 77k + 54k = n + 54 + 131k$$

Постојање броја k таквог да

$$n + 54 + 131k \equiv p(\mod 100)$$

гдје је $p < 100$ прост, слиједи из чињенице да је $(100, 131) = 1$.
Јер то значи да постоје $k, l \in Z$ такви да важи

$$131 \cdot k + 100 \cdot l = 1$$

Одавде је

$$131k \cdot (p - n - 54) \equiv p - n - 54(\mod 100)$$

па за свако p имамо по једно такво k . Доказано. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

295

Нека је n природан број који у систему са основом 2005 има 20 цифара. Ако те цифре, узете неким редом, образују аритметичку прогресију, доказати да је n сложен број.

Доказ. Користићемо следеће тврђење које се лако доказује: Ако је збир цифара неког броја написаног у систему са основом b, $(b > 1)$, дјељив са m и $b-1$ дјељиво са m, тада је и сам број дјељив са m. На примјер, из наведене теореме слиједе критеријуми дјељивости са 3 и 9 у декадном систему.
Нека је n двадесетоцифрен број у систему са основом 2005. Како цифре, узете неким редом, образују аритметичку прогресију, збир цифара броја n је
$a + (a + d) + \cdots + (a + 19d) = 20a + 190d = 2(10a + 95d)$.
Дакле, дјељив је са 2. Међутим, са 2 је дјељиво и $2005 - 1 = 2004$. На основу наведеног тврђења и број n је дјељив са 2. □

(**Јована Шубарић 11/17 Д**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

296

Одредити све уређене парове (x, y) цијелих бројева x и y тако да је $7x^2 - 3y^2 = 17$

Доказ. Нека је $x^2 = a$ и $y^2 = b$. Дата једначина тада је еквивалентна са једначином :

$$7a - 3b = 17$$

гдје је $(a \geq 0, b \geq 0)$. Једно рјешење једначине

$$_0 = 2, b_0 = -1$$

па је опште рјешење једначине $7a - 3b = 17$,дато формулама $a = 3k + 2$,$b = 7k - 1$.
Дакле, $x^2 = 3k + 2$ и $y^2 = 7k - 1$. Како је $x^2 = 3k + 2$, нема рјешење, није могуће да иједан квадрат природног броја при дијељењу са 3 даје остатак 2. □

(**Милош Ћупић 39/18 Д**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/6.%20LINEARNA%20DJ.pdf`

297

Петар и Наташа станују у солитеру у којем на сваком спрату има по 10 станова. Станови почињу од првог спрата и нумерисани су бројевима 1,2,3 итд. Петар станује на спрату чији је број једнак броју стана у којем је Наташа . Збир бројева њихових станова је 239, Који је број стана у којем станује Петар ?

Доказ. Нека Петар станује на спрату $x+1$ гдје је $(x \geq 0)$. Тада је број његовог спрата $10x+y$, гдје је $1 \leq y \leq 10$. Наташа станује у стану број $x+1$.
Према услову задатка је $10x+y+x+1=239$, а то је уствари $11x+y=238$
из чега добијамо да је $11x=238-y$.
Са обзиром на то да је $1 \leq y \leq 10$ једино цјелобројно рјешење ове једначине је $x=21$, $y=7$. Дакле, Петар станује у стану број 217.

□

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

298

На колико начина се 380 динара може подијелити двојици браће , тако да старији добија само нобчанице од 50 динара, а млађи само новчанице од 20 динара?

Доказ. Нека је x број новчаница од 50 динара које треба да добије старији брат , а y број новчаница од 20 динара које треба да добије млађи $(x, y \geq 0)$.Тада је :

$$50x+20y=380$$

можемо скратити ову једначину па имамо : $5x+2y=38$
из овога слиједи да је $2|x$, па нека је $x=2z$, sa неко z. Сада можемо уврстити ово у горњој једначини и мало је средити да добијемо: $5z+y=19$.
Дакле , $5z=19-y \in 0,5,10,15$.
За $z=0$ имамо да је $x=0$ и $y=19$
За $z=1$ имамо да је $x=2$ и $y=14$
За $z=2$ имамо да је $x=4$ и $y=9$
За $z=3$ имамо да је $x=6$ и $y=4$
Значи постоје четири могућности. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

299

Одредити све двоцифрене природне бројеве са особином да је њихова вриједност једнака квадрату збира цифара.

Доказ. Нека је тражени број $\overline{xy}$, при чему је $x \in 1, 2, \ldots, 9$, $y \in 1, 2, \ldots, 9$.
Тада је $(x+y)^2 = 10x + y$. А како је $x + y \neq 0$ добијамо :

$$x + y = \frac{10x + y}{x + y} = 1 + \frac{9x}{x + y}$$

Па $x + y$ може узимати вриједности 1,2,3,9,x,3x,9x. За добијене вриједности је онда $x + y$ такође једнако , редом $1 + 9x$,$1 + 3x$,$1 + x$, 10,4,2.
Дакле , добијамо једначине

$$1 + 9x = 1$$

$$1 + 3x = 3$$

$$1 + x = 9$$

$$10 = x$$

$$4 = 3x$$

$$2 = 9x$$

Од датих једначина једино $1 + x = 9$ гдје је $x = 8$ задовољава услове задатка. Тада је $y = 1$, па је тражени број 81. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

300

Колико природних бројева има особину да је $n^2 + 3n + 24$ потпун квадрат цијелог броја ?

Доказ. Нека је $n^2+3n+24=m^2$. Тада добијемо квадратну једначину:

$$n^2+3n+24-m^2=0$$

Да би n био цио број дискриминанта мора бити потпун квадрат па је :

$$9-4(24-m^2)=k^2$$

Када ово мало средимо добијамо

$$4m^2-k^2=87$$

Односно ово је исто што и

$$(2m-k)(2m+k)=87$$

Могући случајеви су да $2m-k$ узима редом вриједности:

$$1,3,29,87,-1,-3,-29,-87$$

А $2m+k$ редом вриједности □

$$87,29,3,1,-87,-29,-3,-1$$

Одакле је $4m\in 88,32,-88,-32$ тј. $m\in 22,8,-22,-8$, па је $n\in 5,-8,20,-23$.
Како n мора бити природан број онда имамо два рјешења : $n=5$ или $n=20$. (**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

301

Доказати да једначина $x^2+y^2+z^2=2007$ нема рјешења у скупу цијелих бројева.

Доказ. Квадрати цијелих бројева при дијељењу са 4 дају остатак 0 када је број паран и остатак 1 када је број непаран .
Како је $2007\equiv 3(\mod 4)$ сва три броја x,y,z морају бити непарна , тј.
$x=2x_1+1$, $y=2y_1+1$ и $z=2z_1+1$, гдје су x_1,y_1,z_1 такође цијели бројеви. Тада је

$$4x_1^2+4x_1+1+4y_1^2+4y_1+1+4z_1^2+4z_1+1=2007$$

Када средимо ово добијамо израз:

$$x_1(x_1+1)+y_1(y_1+1)+z_1(z_1+1)=501$$

Лијева страна ове једначине је паран број , а десна као што видимо непаран , па једначина нема рјешења у скупу цијелих бројева . □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

302

Доказати да је за сваки природан број n број $n^{13} - n$ дељив са 2730.

Доказ. Како је $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, довољно је доказати да је $n^{13} - n$ дељиво са 2, 3, 5, 7 и 13. По Малој Фермаовој теореми је очигледно дељив са 13. Даље, како је $n^{13} - n = n(n^{12} - 1)$, то се као и у претходном задатку доказује да је дати број дељив са 3. Такође, лако се доказује и да је дати број увек паран. И на крају како је по Малој Фермаовој теореми $n^4 \equiv 1$, уколико n није дељив са 5, то је $n^{12} - 1$ дељив са 5 уколико n није дељив са 5, а ако је дељив са 5 онда је очигледно $n^{13} - n$ дељив са 5. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

303

Нека су дати прости бројеви $p_1 < p_2 < \cdots < p_{31}$. Доказати да ако 30 дели суму њихових четвртих степена, тада међу њима постоје три узастопна проста броја.

Доказ. Докажимо да се међу датим бројевима налазе бројеви 2,3,5.
Наиме, како је четврти степен непарног броја, непаран, то не може свих 31 бројева бити непарно, тј. један од њих мора бити паран. Како је он и прост он мора бити једнак 2. Слично како четврти степени природних бројеви који нису дељиви са 3 дају остатак 1 по модулу 3, то бар неки од датих 31 бројева мора бити дељив са 3. Како је он и прост, он мора бити једнак 3.
Докажимо даље да четврти степен било ког природног броја n који није дељив са 5, даје остатак 1 по модулу 5. Уколико је n конгруентно са 1 или -1 тада је очигледно његов четврти степен конгруентан са 1 по модулу 5. Такође уколико је конгруентан са 2 или -2 тада је његов четврти степен конгруентан са $2^4 = 16$, тј. такође конгруентан са 1 по модулу 5. Сада уколико ниједан од датих 31 бројева није дељив са 5, тада сума њихових четвртих степена даје остатак 1 по модулу 5, што је немогуће. Значи бар једна од њих је дељив са 5, па како је и прост, једнак је 5. □

(**Огњен Пејовић 13/17 Д**) задатак преузет из:
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

304

Доказати да једначина

$$x^2 + y^2 + z^2 + 3(x + y + z) + 5 = 0$$

нема рјешење у скупу рационалних бројева.

Доказ. Дату једначину можемо написати у облику

$$(2x + 3)^2 + (2y + 3)^2 + (2z + 3)^2 = 7$$

Она има рјешења у скупу рационалних бројева ако и само ако постоје цијели бројеви a, b, c, m такви да је :

$$a^2 + b^2 + c^2 = 7m^2$$

Претпоставимо да такви бројеви постоје и нека је m најмање могуће .
Ако је m паран број, $m = 2n$, тада је $a^2 + b^2 + c^2$ дјељиво са 4 и лако се провјерава да тада бројеви a, b, c морају бити парни тј.
$a = 2a_1$,$b = 2b_1$, $c = 2c_1$ и $a_1^2 + b_1^2 + c_1^2 = 7n^2$, што је контрадикција са претпоставком о минималности броја m.Ако је m непаран број тада је $m^2 \equiv 1(\mod 8)$ па је

$$a^2 + b^2 + c^2 \equiv 7(\mod 8)$$

што је немогуће. □

(**Милош Ћупић 39/18 Д**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

305

Пронаћи сва ријешења $x^2 \equiv 1 \pmod{144}$

Доказ. $144 = 16 \cdot 9 = 2^4 3^2$ и нзд$\,16, 9 = 1$
Ову конгруенцију можемо замјенити са двије

$$x^2 \equiv 1 \pmod{16}$$
$$\text{и}$$
$$x^2 \equiv 1 \pmod{9}$$

$x^2 \equiv 1 \pmod{16}$ има четири ријешења: $x \equiv \pm 1 \pm 7 \pmod{16}$
$x^2 \equiv 1 \pmod{9}$ има два ријешења: $x \equiv \pm 1 \pmod{9}$
Постоји осам могућности

(i) $x \equiv 1 \pmod{16} \wedge x \equiv 1 \pmod{9}$

(ii) $x \equiv 1 \pmod{16} \wedge x \equiv -1 \pmod{9}$

(iii) $x \equiv -1 \pmod{16} \wedge x \equiv 1 \pmod{9}$

(iv) $x \equiv -1 \pmod{16} \wedge x \equiv -1 \pmod{9}$

(v) $x \equiv 7 \pmod{16} \wedge x \equiv 1 \pmod{9}$

(vi) $x \equiv 7 \pmod{16} \wedge x \equiv -1 \pmod{9}$

(vii) $x \equiv -7 \pmod{16} \wedge x \equiv 1 \pmod{9}$

(viii) $x \equiv -7 \pmod{16} \wedge x \equiv -1 \pmod{9}$

По кинеској теореми о остацима када је $k = 2$, $m_1 = 16$ и $m_2 = 9$, сваки горе наведени случај има јединствено рјешење за x по модулу 144.
Рачунамо:
$z_1 = m_2 = 9$
$z_2 = m_1 = 16,$

$y_1 \equiv 9^{-1} \equiv 9 \pmod{16}$
$y_2 \equiv 16^{-1} \equiv 4 \pmod{9}$

$w_1 \equiv 9 \cdot 9 = 81 \pmod{144}$
$w_2 \equiv 16 \cdot 4 \equiv 64 \pmod{144}$

Осам рјешења су:

(i) $x \equiv 1 \cdot 81 + 1 \cdot 64 \equiv 145 \equiv 1 \pmod{144}$

(ii) $x \equiv 1 \cdot 81 + (-1) \cdot 64 \equiv 17 \equiv 17 \pmod{144}$

(iii) $x \equiv (-1) \cdot 81 + 1 \cdot 64 \equiv -17 \equiv -17 \pmod{144}$

(iv) $x \equiv (-1) \cdot 81 + (-1) \cdot 64 \equiv -145 \equiv -1 \pmod{144}$

(v) $x \equiv 7 \cdot 81 + 1 \cdot 64 \equiv 631 \equiv 55 \pmod{144}$

(vi) $x \equiv 7 \cdot 81 + (-1) \cdot 64 \equiv 503 \equiv 71 \pmod{144}$

(vii) $x \equiv (-7) \cdot 81 + 1 \cdot 64 \equiv -503 \equiv -71 \pmod{144}$

(viii) $x \equiv (-7) \cdot 81 + (-1) \cdot 64 \equiv -603 \equiv -55 \pmod{144}$

□

(**Јакша Мрдак 23/17 Д**)

306

Нека је дате двије линеарне конгруенције
$x \equiv 2 \pmod{24}$
$x \equiv 8 \pmod{39}$

Доказ. Нека је сада $x = 2+24r = 8+39s$ из чега слиједи $24r-39s = 6$. Како је $(24, 39) = 3$ те како 3 дијели 6, имамо рјешење. Аналогним поступком долазимо до једнакости $39\cdot 2-24\cdot 3 = 6$ па тако слиједи $x = 2 + 24 \cdot (-3) = -70$.

Опште рјешење је $x = -70 + [24, 39]k, k \in$.

Како је $[24, 39] = 312$, слиједи да су рјешења облика $x = -70 + 312k, k \in$, односно $x \equiv -70 \pmod{312}$.

Из тога слиједи како је $x = -70 + 312 = 242$ најмање позитивно рјешење.

□

(Јакша Мрдак 23/17 Д)

307

Одредимо број природних бројева који су релативно прости с бројем 10^{100} и мањи су од њега.

Доказ. Требамо одредити $\phi(10^{100})$.

$\phi(10^{100}) = \phi(2^{100} \cdot 5^{100}) = 2^{99} \cdot 5^{99} \cdot 4 = 4 \cdot 10^{99}$.

□

(Јакша Мрдак 23/17 Д)

308

Одредити сва решења једначине 4x +5y = 100 ако су x и y цели бројеви.

Доказ. Прво очигледно решење ове једначине је за

X0 = 0, y0 = 20.

(x0, y0)= (0, 20)

добијамо:

x = 5к и y = 20 − 4к .

Решење за y можемо добити и ако уместо x у почетну једначину ставимо x = 5к :

4 *5к + 5y =100

20к + 5y =100 ,

поделимо леву и десну страну једначине са 5

4к + y = 20

y = 20 − 4к .

Решење ове једначине је уређени пар (x,y) = (5к;20 − 4к), (к ∈ Ɜ)

□

(Јакша Мрдак 23/17 Д)

309

Колико има парова природних бројева (x,y) таквих да је 4x +7y = 2005?

Доказ. У овој једначини видимо да 2005 није дељив са 4 па се морамо мало помучити да нађемо почетно решење.

Како је 4x = 2005 − 7 y , видимо да 2005 − 7y мора бити дељив са 4.
За y=0
2005 − 0 = 2005 , није дељив са 4
За y = 1
2005 − 7 = 1998 , није дељив са 4
За y = 2
2005 − 14 = 1991, није дељив са 4
За y = 3
2005 − 21 = 1984 , је дељив са 4, јер је 1984 : 4 = 496.

Сада имамо почетно решење (x0, y0)= (496, 3) јер је:
4x + 7 y = 2005
4 * 496 + 7 * 3 = 2005.
Како је 4x + 7 y = 2005

x = x0 − 6к	y = y0 + ак
x = 496 − 7к	y = 3 + 4к
496 − 7к > 0	3 + 4к > 0
7к < 496	4к > − 3
к ≤ 70	к ≥ 0

$$0 \leq к \leq 70$$

Постоји тачно 71 решење тј. постоји тачно 71 уређени пар који задовољавају ову једначину.

□

(**Јакша Мрдак 23/17 Д**)

310

Решимо почетни проблем који можемо записати као систем конгруенција $x \equiv 2 \pmod 3, x \equiv 3 \pmod 5, x \equiv 2 \pmod 7$.

Доказ. Имамо: $a_1 = 2, m_1 = 3, a_2 = 3, m_2 = 5, a_3 = 2, m_3 = 7$.
Видимо да је (3,5) = 1, (3,7) = 1, (5,7) = 1.
$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$
$n_1 = \frac{m}{m_1} = \frac{105}{3} = 35, n_2 = \frac{m}{m_2} = \frac{105}{5} = 21, n_3 = \frac{m}{m_3} = \frac{105}{7} = 15$

$$\begin{aligned} n_1 x &\equiv a_1 \pmod{m_1} \\ 35x &\equiv 2 \pmod 3 \\ 2x &\equiv 2 \pmod 3 \\ &\Rightarrow x_1 = 1 \end{aligned}$$

$$\begin{aligned} n_2 x &\equiv a_2 \pmod{m_2} \\ 21x &\equiv 3 \pmod 5 \\ x &\equiv 3 \pmod 5 \\ &\Rightarrow x_2 = 3 \end{aligned}$$

$$\begin{aligned} n_3 x &\equiv a_3 \pmod{m_3} \\ 15x &\equiv 2 \pmod 7 \\ x &\equiv 2 \pmod 7 \\ &\Rightarrow x_3 = 2 \end{aligned}$$

Рјешење проблема је:

$$\begin{aligned} x &= 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2 \pmod{105} \\ &= 35 + 63 + 30 \pmod{105} \\ &= 128 \pmod{105} \\ &= 23 \pmod{105} \end{aligned}$$

□

(**Никола Цупара 08/17 Д**) http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/BIN01.pdf

311

Решити једначину $17x + 11y = 20$.

Доказ. Прво испитујемо да ли једначина има решење, а има га ако $(17, 20)|20 \Leftrightarrow 1|20$, одакле следи да једначина има решење.
У овом случају тражимо партикуларно решење, и то помоћу Еуклидовог алгоритма.

$$\begin{aligned} 17 &= 11 \cdot 1 + 6 \\ 11 &= 6 \cdot 1 + 5 \\ 6 &= 5 \cdot 1 + 1 \\ 5 &= 1 \cdot 5 \end{aligned}$$

Сада имамо (због $d = \alpha a + \beta b$) (последица Еуклидовог алгоритма)
$1 = 6 - 5 = 6 - (11 - 6) = 2 \cdot 6 - 11 = 2 \cdot (17 - 11) - 11 = 2 \cdot 17 - 3 \cdot 11$
Дакле, $\alpha = 2$ и $\beta = -3$.
Сада, $q = \frac{c}{d} = \frac{20}{1} = 20$, па је партикуларно решење:

$$\begin{aligned} x_0 &= \alpha q = 2 \cdot 20 = 40 \\ y_0 &= \beta q = -3 \cdot 20 = -60 \end{aligned}$$

Када смо нашли партикуларно решење напишимо опште решење једначине:

$$\begin{aligned} x &= x_0 + \frac{b}{d}t = 40 + \frac{11}{1}t = 40 + 11t \\ y &= y_0 - \frac{a}{d}t = -60 - \frac{17}{1}t = -60 - 17t \end{aligned}$$

□

(**Никола Цупара 08/17 Д**) https://www.scribd.com/document/375050244/Teorija-brojeva-radna-ver

312

Испитати да ли линеарна Диофантова једначина $13x + 32y = 5$ има рјешење.

Доказ. Прво провјеравамо да ли нзд$(13, 32) \mid 5$. Користећи Еуклидов алгоритам добијамо:

$$\begin{aligned} 32 &= 2 \cdot 13 + 6 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 6 \cdot 1. \end{aligned}$$

Дакле, једначина има рјешење јер је нзд$(13, 32) = 1$ и $1|5$.

□

(**Никола Цупара 08/17 Д**) `https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic.pdf`

313

За превоз неке робе располажемо врећама од 40кг и 60кг. Колико треба узетих и једних и других врећа да се превезе 500кг робе?

Доказ. Поставимо једначину
$40x + 60y = 500$, гдје је x број врећа од 40кг, а y број врећа од 60кг.
Како су x и y ненегативни цијели бројеви, то је ова једначина Диофантова линеарна једначина.
Дакле, решавамо једначину

$$\begin{aligned} 40x + 60y = 500 &| : 20 \\ 2x + 3y &= 25 \end{aligned}$$

Како је $1 = (2, 3), 1|5$ следи да једначина има решење.
Одредимо једно решење дате једначине "напамет"(јер су мали коефицијенти).
Видимо да је $x_0 = 5$ и $y_0 = 5$.
Општа решења једначине гласе:
$x = 5 + 3t, y = 5 - 2t$
Уважимо још услов да су $x, y \geq 0$.

$$\begin{aligned} x \geq 0 \Rightarrow 5 + 3t \geq 0 \Rightarrow 3t \geq -5 \Rightarrow t \geq \frac{-5}{3} \\ y \geq 0 \Rightarrow 5 - 2t \geq 0 \Rightarrow 2t \geq 5 \Rightarrow t \geq \frac{5}{2} \end{aligned}$$

Дакле, $\frac{-5}{3} \leq t \leq \frac{5}{2} \Rightarrow t \in \{-1, 0, 1, 2\}$
За ове вредности броја t, имамо решења:
$(x, y) \in \{(2, 7), (5, 5), (8, 3), (11, 1)\}$. □

(**Никола Цупара 08/17 Д**) https://www.scribd.com/document/375050244/Teorija-brojeva-radna-ver

314

Доказати да за сваки непаран број n важи $n \mid 2^{n!} - 1$.

Доказ. За све природне бројеве n имамо да важи $\varphi(n) \mid n!$. Заправо, то је тачно за $n = 1$. Ако је $n > 1$ и ако је $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$, тако да је $q_1 < q_2 < \ldots < q_k$, онда

$$\varphi(n) = q_1^{\alpha_1 - 1} q_2^{\alpha_2 - 1} \cdots q_k^{\alpha_k - 1} (q_1 - 1) \cdots (q_k - 1)$$

и имамо $q_1^{\alpha_1 - 1} q_2^{\alpha_2 - 1} \cdots q_k^{\alpha_k - 1} \mid n$, $q_1 - 1 < q_k \leq n$, одакле слиједи да су $q_k - 1 < n$ и $q_1 - 1 < q_2 - 1 < \ldots < q_k - 1$ различити природни бројеви мањи од n. Тако да $q_1 - 1 \cdot q_2 - 1 \cdots q_k - 1 \mid (n-1)!$. То значи да $\varphi(n) \mid (n-1)! \cdot n = n!$.
Ако је n непаран, онда на основу Ојлерове теореме слиједи $n \mid 2^{\varphi(n)-1} \mid 2^{n!} - 1$ и тиме је доказ завршен.

□

(**Никола Цупара 08/17 Д**) задатак преузет са
https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf

315

Наћи остатак при дељењу 317^{259} са 15.

Доказ. $317 \equiv 2 \pmod{15} \Rightarrow 317^{259} \equiv 2^{259} \pmod{15}$
Како је (2,15) = 1, на основу Ојлерове теореме следи :

$$(2^{\phi})^{(15)} \equiv 1 \pmod{15}$$
$$\phi(15) = \phi(5) \cdot \phi(3) = 4 \cdot 2 = 8$$
$$2^8 \equiv 1 \pmod{15}$$
$$259 = 8 \cdot 32 + 3 \Rightarrow 2^{259} = (2^8)^{32} \cdot 2^3 \Rightarrow 2^{259} \equiv (2^8)^{32} \cdot 2^3 \pmod{15}$$

Одавде слиједи, због $2^8 \equiv 1 \pmod{15}$,
$2^{259} \equiv 2^3 \pmod{15}$, односно, остатак је 8. □

(**Никола Цупара 08/17 Д**) https://www.scribd.com/document/375050244/Teorija-brojeva-radna-ver

316

Одредити последњу цифру производа првих сто природних бројева који при дељењу са 5 дају остатак 3.

Доказ. Сви природни бројеви који приликом дељења са 5 дају остатак 3 могу се записати у облику $5k+3, k \in N_0$. Запишимо производ првих сто таквих бројева:

$$3 \cdot 8 \cdot 13 \cdot 18 \cdot 23 \cdot 28 \cdot 33 \cdots (5k+3) \cdots 498 =$$
$$(3 \cdot 8) \cdot (13 \cdot 18) \cdot (23 \cdot 28) \cdot (33 \cdots 38) \cdots ((5k-2) \cdot (5k+3)) \cdots (493 \cdot 498).$$

Сваки од 50 производа у заградама завршава цифром 4. Заиста,

$$n = (5k-2)(5k+3) \equiv -6 \equiv 4 \pmod 5,$$

те је очито n паран јер је $5k+3-(5k-2) = 5$. Према, Кинеској теореми о остацима, систем конгруенција

$$n \equiv 4 \pmod 5, n \equiv 0 \pmod 2,$$

има јединствено решење модуло 10, па је то нпр. 4, а сва су решења $n \equiv 4 \pmod{10}$
Задња цифра нашег производа је задња цифра потенције 4^{50}. Како је $4^{50} = 16^{25}$, а потенције броја 16 увек завршавају цифром 6, па тражени производ завршава управо цифром 6. □

(**Никола Цупара 08/17 Д**) `https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

317

Решити систем линеарних конгруенција

$$x \equiv 1 \pmod 7,$$
$$x \equiv 3 \pmod 4,$$
$$x \equiv 9 \pmod{15}.$$

Доказ. Како је $m_1 = 7, m_2 = 4 = 2 \cdot 2$ и $m_3 = 15 = 3 \cdot 5$, то су модули у паровима релативно прости па можемо применити Кинеску теорему о остацима за решавање добијеног система.

$$M = m_1 \cdots m_2 \cdot m_3 = 7 \cdot 4 \cdot 15 = 420$$

$$n_1 = \frac{M}{m_1} = \frac{420}{7} = 60$$
$$n_2 = \frac{M}{m_2} = \frac{420}{4} = 105$$
$$n_3 = \frac{M}{m_3} = \frac{420}{15} = 28$$

Да бисмо дошли до решења система потребно је да решимо следеће три линеарне конгруенције:

$$60x_1 \equiv 1 \pmod 7,$$
$$105x_2 \equiv 3 \pmod 4,$$
$$28x_3 \equiv 9 \pmod{15}.$$

Скратимо конгруенције по одговарајућим модулима ($60 \equiv 4 \pmod 7, 105 \equiv 1 \pmod 4, 28 \equiv 13 \pmod{15}$) добијамо следеће конгруенције:

$$\begin{aligned} 4x_1 &\equiv 1 \pmod 7, \\ x_2 &\equiv 3 \pmod 4, \\ 13x_3 &\equiv 9 \pmod{15}. \end{aligned}$$

Решимо ли сваку конгруенцију посебно, добијамо следеће резултате:

$$\begin{aligned} x_1 &\equiv 2 \pmod 7, \\ x_2 &\equiv 3 \pmod 4, \\ x_3 &\equiv 3 \pmod{15}. \end{aligned}$$

Сада је решење полазног система:

$$\begin{aligned} x &\equiv n_1 \cdot x_2 + n_2 \cdot x_2 + n_3 \cdot x_3 \pmod M \\ &\equiv 60 \cdot 2 + 105 \cdot 3 + 28 \cdot 3 \pmod{420} \\ &\equiv 519 \pmod{420} \\ &\equiv 99 \pmod{420} \end{aligned}$$

□

(**Никола Цупара 08/17 Д**) `http://www.math.pitt.edu/~sparling/081/10281/10281quizzes/10281e2s.pdf`

318

Решити систем конгруенција

$$\begin{aligned} 11x &\equiv 13 \pmod{20} \\ 9x &\equiv 17 \pmod{25} \end{aligned}$$

Доказ. Прво ћемо решити $11x \equiv 13 \pmod{20}$. Приметимо да је $11 \cdot 11 = 121 \equiv 1 \pmod{20}$, па

$$x = 13 \cdot 11 \equiv 143 \equiv 3 \pmod{20}.$$

Након тога решавамо $9x \equiv 17 \pmod{25}$. Приметимо да је $9 \cdot 11 \equiv -1 \pmod{25}$, па

$$x \equiv -17 \cdot 11 \equiv 8 \cdot 11 \equiv 88 \equiv 13 \pmod{25}.$$

Стога је почетни систем еквивалентан

$$\begin{aligned} x &\equiv 3 \pmod{20} \\ x &\equiv 13 \pmod{25}. \end{aligned}$$

Или, како смо закључили да је прва конгруенција еквивалентна $x \equiv 3 \pmod{20}$, можемо направити смјену $x = 3 + 20k$ у другу смјену како би добили

$$9(3 + 20k) \equiv 17 \pmod{25}$$

те поједноставити да добијемо

$$5k \equiv -10 \pmod{25},$$

које за решење има $k = 3, x = 3 + 20 \cdot 3 = 63$. Након што пронађемо једно решење, тада је због $[25, 20] = 100$ опште решење дато са

$$x \equiv 63 \pmod{100}.$$

□

(**Никола Цупара 08/17 Д**) задатак преузет са:
`http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/TOB02.pdf`

319

Одредити све природне бројеве n за које је $\phi(n)$ непаран број.

Доказ. Из дефиниције Ојлерове функције знамо да је $\phi(1) = 1$, па је $\phi(2) = 1$, јер

$$\phi(n) = n \cdot \prod_{i=1}^{k}(1 - \frac{1}{p_i})$$

је Ојлерова функција, одакле смо и закључили да је $\phi(2) = 2 \cdot (1 - \frac{1}{2}) = 1$. Претпоставимо да је $n > 2$. Ако постоји непаран фактор p_i од n, онда је $p_i - 1$ паран број, па је ϕ паран број због следеће формуле:

$$\phi = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{k}(1 - \frac{1}{p_i})$$

из које добијамо да ће у једном чиниоцу функције $\phi(n)$ бити $\frac{p_i - 1}{p_i}$. Ако не постоји непаран фактор p_i од n, онда је $n = 2^{\alpha}$, $\alpha \geq 2$, па је

$$\phi(n) = 2^{\alpha - 1}(2 - 1) = 2^{\alpha - 1}.$$

Како је $\alpha - 1 \geq 1$, слиједи да је $\phi(n)$ паран број. Закључујемо да је $\phi(n)$ непаран број само за $n \in \{1,2\}$.

□

(**Никола Цупара 08/17 Д**) задатак преузет са:
`http://e.math.hr/Vol31/Bokun#e10`

320

Ако је n непаран цијели број, тада је $\phi(2n) = \phi(n)$. Доказати.

Доказ. Како је n непаран број, онда дати израз можемо записати на сљедећи начин:

$$\phi(2n) = \phi(2) \cdot \phi(n)$$

Знамо да је $\phi(2) = 1$, па је:

$$\phi(2) \cdot \phi(n) = 1 \cdot \phi(n) = \phi(n)$$

Добијамо да је $\phi(2n) = \phi(n)$, па смо овим завршили наш доказ.

□

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/TOB02.pdf`

321

Пронаћи опште рјешење система:

$$\begin{aligned} x &\equiv 2 \pmod{12} \\ x &\equiv 8 \pmod{10} \\ x &\equiv 9 \pmod{13} \end{aligned}$$

Доказ. Прво рјешавамо прве двије конгруенције: тражимо x тако да је $x = 2+12r = 8+10s$. Једноставно се доказује да је $x = 38$ рјешење. Како је НЗС$[12, 10] = 60$, опште рјешење прве двије конгруенције једнако је $x = 38 + 60k$ за $k \in Z$. Тако је рјешење система прве 3 конгруенције једнако рјешењу система:

$$\begin{aligned} x &\equiv 38 \pmod{60} \\ x &\equiv 9 \pmod{13} \end{aligned}$$

Овај пар конгруенција има својство да је модуо 13 у трећој конгруенцији почетног система мањи од модуа 60 којег добијамо из прве двије конгруенције. Треба наћи неко t такво да је $x = 38 + 60t = 9 + 13u$ за неко u, а то постижемо постављајући конгруенцију:

$$38 + 60t \equiv 9 \pmod{13}$$

која се другачије може записати и овако

$$-1 - 5t \equiv 9 \pmod{13}$$

што даље даје

$$-5t \equiv 10 \pmod{13}$$

те добијамо

$$t \equiv -2 \equiv 11 \pmod{13}$$

па је онда $x = 38 + 60 \cdot (11) = 698$

Како је НЗС$[12, 10, 13] = 60 \cdot 13 = 780$, онда је опште рјешење почетне три конгруенције:

$$x \equiv 698 \pmod{780}$$

□

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/TOB02.pdf`

322

Одредити све троцифрене природне бројеве који су дјељиви са 7, а при дијељењу са 9 дају остатак 5.

Доказ. Из поставке задатка слиједи:

$$n = 7x \text{ и } n = 9y + 5, x, y \in N$$

Рјешавамо диофантову једначину $7x = 9y + 5$, тј.

$$7x - 9y = 5$$

Како НЗД$(7, 9) \mid 5$, ова једначина има рјешење.

Једно рјешење ове једначине је $x_0 = 2$ и $y_0 = 1$. Тада је опште рјешење $x = 2 + 9t, y = 1 + 7t, t \in N$.

Како је $100 < n < 1000$, а $n = 7x = 14 + 63t$, важи да је:

$$\begin{aligned} 100 < 14 + 63t < 1000 \\ 86 < 63t < 986 \\ 1.3 < t < 15.6 \end{aligned}$$

па је $t \in \{2, 3, 4, \ldots, 15\}$. Стога закључујемо да је:

$$n = 14 + 63t, t \in \{2, 3, 4, \ldots, 15\}$$

или

$$n \in \{140, 203, 266, 329, 392, 455, 518, 581, 644, 707, 770, 833, 896, 959\}$$

□

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

323

Наћи сва рјешења система једначина $x + y + z = 3$ и $x^3 + y^3 + y^3 = 3$.

Доказ. Из поставке имамо да је:

$$(x + y + z)^3 - (x^3 + y^3 + z^3) = 3(x + y)(x + z)(y + z)$$

Дакле, ако су x, y и z цијели бројеви такви да $x + y + z = 3$ и $x^3 + y^3 + z^3 = 3$ онда из прве једначине добијамо

$$8 = (x + y)(x + z)(y + z) = (3 - x)(3 - y)(3 - z)$$

а из $x+y+z=3$ имамо да је

$$6=(3-x)+(3-y)+(3-z)$$

Трећа једначина показује да су сва три броја $3-x, 3-y, 3-z$ непарни или је само један од њих непаран.

У првом случају, из друге једначине сви ови бројеви су једнаки $|2|$ а самим тим из треће закључујемо да су једнаки 2 и онда је $x=y=z=1$.

У другом случају, из друге једначине закључујемо да је један од бројева $3-x, 3-y, 3-z$ једнак $|8|$, а остали су једнаки $|1|$. Узмимо то у обзир и из треће једначине закључујемо да је један од њих 8 а друга два су -1.

Одавде слиједи да је $x=-5, y=z=4; x=y=4, z=-5$ или $x=z=4, y=-5$.

Овим закључујемо да овај систем једначина има само 4 могућа рјешења и то су:

$$\begin{aligned} x,y,z &= 1,1,1 \\ x,y,z &= -5,4,4 \\ x,y,z &= 4,-5,4 \\ x,y,z &= 4,4,-5 \end{aligned}$$

□

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`https://www.academia.edu/2991414/Uvod_u_teoriju_brojeva_skripta_?auto=download`

324

Нека је p прост број и $p \equiv 1 \pmod 4$. Доказати да тада једначина $x^2 - py^2 = -1$ има рјешења.

Доказ. Нека је (x_1, y_1) најмање рјешење једначине $x^2 - py^2 = 1$. Тада је x_1 непаран а y_1 паран.

Из

$$\frac{x_1-1}{2} \cdot \frac{x_1+1}{2} = p \cdot (\frac{y_1}{2})^2$$

и

$$(\frac{x_1-1}{2}, \frac{x_1+1}{2}) = 1$$

слиједи да постоје $u, v \in N$ такви да је:

$$\frac{x_1 \pm 1}{2} = pu^2, \frac{x_1 \pm 1}{2} = v^2, \frac{y_1}{2} = uv$$

Одавде је $v^2 - pu^2 = \pm 1$.

Из $u < y_1$ слиједи да овдје не можемо имати предзнак тј важи да је $v^2 - pu^2 = -1$. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

325

Наћи најмањи природан број x за који је $x \equiv 5 \pmod 7, x \equiv 7 \pmod{11}, x \equiv 3 \pmod{13}$.

Доказ. Како су $7, 11$ и 13 узајамно прости бројеви, овим су услови Кинеске теореме о остацима задовољени.

Имамо да је $a_1 = 5, a_2 = 7, a_3 = 3; m_1 = 7, m_2 = 11, m_3 = 13; m = 7 \cdot 11 \cdot 13 = 1001$.

$\frac{m}{m_j}$ је цијели број и $(\frac{m}{m_j}, m_j) = 1$ за $1, 2, 3$.

$\frac{m}{m_1} = 143, \frac{m}{m_2} = 91$ и $\frac{m}{m_3} = 77$

Важно је напоменути да ако је $(a, m) = 1, a, m \in N$, конгруенција $ax \equiv b \pmod m$ увијек има рјешење.

Рјешење је $x = b \cdot a^{\varphi(m)-1}$. На основу Ојлерове теореме је:

$$ax - b = a \cdot b \cdot a^{\varphi(m)-1} - b = b(a^{\varphi(m)} - 1) \equiv 0 \pmod m$$

Према томе, за свако $j = 1, 2, 3$ постоје цијели бројеви b_j такви да је $\frac{m}{m_j} \cdot b_j \equiv 1 \pmod{m_j}$. Јасно је да важи $\frac{m}{m_j} \cdot b_j \equiv 0 \pmod{m_i}$ за $i \neq j$.

Одредимо b_1, b_2, b_3 у нашем случају.

а) $143b_1 \equiv 1 \pmod 7$, тј. $3b_1 \equiv 1 \pmod 7$, па је:

$$b_1 \equiv 3^{\varphi(7)-1} \equiv 3^{6-1} \equiv 243 \equiv 5 \pmod 7$$

б) $91b_2 \equiv 1 \pmod{11}$, тј. $3b_2 \equiv 1 \pmod{11}$, па је:

$$b_2 \equiv 3^{\varphi(11)-1} \equiv 3^{10-1} \equiv (3^3)^3 \equiv 5^3 \equiv 4 \pmod{11}$$

в) $77b_3 \equiv 1 \pmod{13}$, тј. $-b_1 \equiv 1 \pmod{13}$, па је:

$$b_3 \equiv -1 \pmod{13}$$

Нека је $x_0 = \sum_{j=1}^{3} \frac{m}{m_j} b_j a_j$. Тада је:

$$x_0 \equiv \frac{m}{m_i} b_i a_i \equiv a_i \pmod{m_i}, i = 1, 2, 3$$

па је x_0 рјешење датог система конгруенција.

$$x_0 = 143 \cdot 5 \cdot 5 + 91 \cdot 4 \cdot 7 + 77 \cdot (-1) \cdot 3 = 5892 = 5 \cdot 1001 + 887$$

па је 887 најмањи природан број који задовољава дати систем конгруенција. □

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`http://web.math.ucsb.edu/~agboola/teaching/2005/winter/old-115A/sol3.pdf`

326

Израз $\phi(3n) = 3\phi(n)$ је тачан ако и само ако $3 \mid n$. Доказати.

Доказ. Претпоставимо да $3 \nmid n$. То значи да је $\text{нзд}(3, n) = 1$. Тада можемо дати израз можемо раставити на сљедећи начин:

$$\phi(3n) = \phi(3) \cdot \phi(n) = 2 \cdot \phi(n)$$

Како $\phi(3n) \neq 2\phi(n)$ из тога слиједи $\implies 3 \mid n$.

Сада кад знамо да $3 \mid n$, докажимо да за у овом случају важи $\phi(3n) = 3\phi(n)$.
Дакле, $3 \mid n$, па на основу тога број n можемо записати као производ степена броја 3 и неког броја m:

$$n = 3^k \cdot m$$

, при чему је $\text{нзд}(3, m) = 1$, односно $3 \nmid n$. Сада n замијенимо добијеним изразом, па имамо:

$$\phi(3n) = \phi(3^k \cdot 3 \cdot m) = \phi(3^{k+1} m)$$

Добијену Ојлерову функцију можемо раставити на производе двије нове:

$$\phi(3^{k+1} m) = \phi(3^{k+1}) \cdot \phi(m)$$

Израз $\phi(3^{k+1})$ можемо даље сређивати:

$$\phi(3^{k+1}) = 3^{k+1} - 3^k = 3(3^k - 3^{k-1})$$

Вратимо се у претходни израз и замијенимо $\phi(3^{k+1})$ са добијеним изразом:

$$3(3^k - 3^{k-1}) \cdot \phi(m) = 3\phi(3^k) \cdot \phi(m) = 3\phi(3^k m)$$

Како је $3^k m = n$, то замијенимо у изразу и имамо:

$$3\phi(3^k m) = 3\phi(n)$$

Тако смо доказали да је $\phi(3n) = 3\phi(n)$.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`http://web.math.ucsb.edu/~agboola/teaching/2005/winter/old-115A/sol3.pdf`

327

Израз $\phi(n) = n/2$ је тачан ако и само ако $n = 2^k$ за неко $k \geq 0$. Доказати.

Доказ. Претпоставимо да је $\phi(n) = n/2$ и запишимо n у сљедећем облику: $n = 2^k N$, гдје је N непаран број. Тада је:

$$n/2 = \phi(n) = \phi(2^k N) = \phi(2^k) \cdot \phi(N) =$$

$$= 2^{k-1} \cdot \phi(N)$$

Добили смо да је $n/2 = 2^{k-1} \cdot \phi(N)$. Сада све помножимо са 2 и добијамо:

$$2 \cdot n/2 = 2 \cdot 2^{k-1} \cdot \phi(N)$$

$$n = 2^k \cdot \phi(N)$$

Сада имамо да је $n = 2^k \cdot \phi(N)$ и $n = 2^k \cdot N$ из чега слиједи $\implies N = \phi(N)$. То значи да како је N непаран број, и $\phi(N)$ је непаран број. Како је $\phi(N)$ непаран број, из тога слиједи $\implies N = 1$.

Претпосавимо обратно, да је $n = 2^k$. Тада имамо да је:

$$\phi(n) = \phi(2^k) = 2^{k-1}$$

Средимо још мало израз и добијамо:

$$2^{k-1} = 2^k/2 = n/2$$

Овим смо доказали наше тврђење.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`http://web.math.ucsb.edu/~agboola/teaching/2005/winter/old-115A/sol3.pdf`

328

Доказати да је n прост број ако и само ако је $\phi(n) = n - 1$.

Доказ. Претпоставимо да је n прост број. То значи да је сваки позитиван цијели број x мањи од релативно прост са n, односно нзд$(n, x) = 1$, а како тих бројева има $n - 1$, из тога слиједи $\implies \phi(n) = n - 1$.

Претпоставимо да је $\phi(n) = n - 1$ и да n није прост број. Број n можемо записати у облику прозвода неких бројева a и b: $n = ab$. Како n има бар два дјелиоца, а са свим осталим

позитивним цијелим бројевима мањим од себе је релативно прост, тих бројева има највише $n-1-2$, па је:

$$\phi(n) \leq n-1-2 \implies \phi(n) \leq n-3 \implies \phi(n) < n-2$$

Видимо да $\phi(n) \neq n-1$, па закључујемо да n мора да буде прост број.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://math.berkeley.edu/~arash/55/55su16q2.pdf`

329

Наћи све парове природних бројева a,b за које важи $2^a + 17 = b^4$

Доказ. Посматрајмо једначину по модулу 17
Из $2^{4a} \equiv b^{16} \equiv 1 \pmod{17}$ слиједи да $8 \mid 4a$,тј. $2 \mid a$, па је $17 = (b - 2^{\frac{a}{2}})(b + 2^{\frac{a}{2}})$. Одавде долазимо до јединог решења $(a, b) = (6, 9)$ □

(**Николина Јеловац 13/18 Д**) задатак преузет са
`https://imomath.com/srb/dodatne/32zadatka_2014_IMO-pripreme_ddj.pdf`

330

Нека су a и b узајамно прости непарни природни бројеви. Наћи све могуће вриједности броја нзд$(2^a + 2^{\frac{a+1}{2}} + 1, 2^b + 2^{\frac{b+1}{2}} + 1)$

Доказ. Примјетимо да је:
$(2^a + 2^{\frac{a+1}{2}} + 1)((2^a - 2^{\frac{a+1}{2}} + 1) = (2^a + 1)^2 - 2^{a+1} = 2^{2a} + 1$
Слиједи да је:
$d = (2^a + 2^{\frac{a+1}{2}} + 1, 2^b + 2^{\frac{b+1}{2}} + 1) \mid (2^{2a} + 1, 2^{2b} + 1) \mid (2^{4a} - 1, 2^{4b} - 1) = 2^{(4a,4b)} - 1 = 15.$
Притом $3 \nmid 2^{2a} + 1$, па имамо $d \mid 5$. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
`https://imomath.com/srb/dodatne/32zadatka_2014_IMO-pripreme_ddj.pdf`

331

Ако је p> 2 прост број и a $\in \mathbb{Z}$, доказати да сваки прост дјелилац q броја $\frac{a^p-1}{a-1} = a^{p-1} + a^{p-2} + \cdots + 1$ задовољава $p \mid q - 1$ или p=q.

Доказ. Ако $q \mid a - 1$ онда $q \mid a^{p-1} + a^{p-2} + \cdots + 1 \equiv 1 + 1 + \cdots + 1 = p \pmod{q}$ дакле q=p.
С друге стране,ако је $q \nmid a - 1$, поредак броја a по модулу q дијели p,дакле једнак је p.
Како тај поредак дијели $q - 1$, слиједи $p \mid q - 1$. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imomath.com/srb/dodatne/stepene%20kongruencije_ddj.pdf

332

Доказати да се бројеви 1,2,...,100 могу распоредити у поља таблице 10x10 тако да су у сваком квадрату 2x2 производи по два броја по дијагонали једнаки по модулу 101.

Доказ. Нека је g примитивни коријен по модулу 101. Упишимо у поље i-те и j-те колоне $(i, j \in \{0, 1, ..., 9\})$ остатак g^{10i+j} при дијељењу са101. У сваком квадрату одређеном врстама i,i+1 и колонама j,j+1, производ бројева по свакој дијагонали је $g^{10(2i+1)+(2j+1)} \pmod{101}$ □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imomath.com/srb/dodatne/stepene%20kongruencije_ddj.pdf

333

Наћи све парове простих бројева p,q за које $pq \mid (5^p - 2^p)(5^q - 2^q)$.

Доказ. Јасно је да су p и q непарни. Примјетимо да ако $p \mid 5^p - 2^p \equiv 3 \pmod{p}$,онда је p=3. Претпоставимо да је p=3(аналогно за q=3). Тада $3q \mid (5^3-2^3)(5^q-2^q) = 3^2 \cdot 13(5^q-2^q)$,одакле је p=3 или q=13.
Претпоставимо сада да је $p > q > 3$. Тада $p \mid 5^q - 2^q$ и $q \mid 5^p - 2^p$. Како $q \mid 5^{q-1} - 2^{q-1}$, важи $5^n \equiv 2^n \pmod{q}$ sa све n дјељиве са q-1 или са p.
При том су q-1 и p узајамно прости,па постоје x,y ∈ ℕ за које је $px = (q-1)y + 1$.
Тада је $5 \cdot 2^{(q-1)y} \equiv 5 \cdot 5^{(q-1)y} = 5^{px} \equiv 2^{px} = 2 \cdot 2^{(q-1)y} \pmod{q}$, одакле $q \mid 3 \cdot 2^{(q-1)y}$, што је контрадикција. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imomath.com/srb/dodatne/stepene%20kongruencije_ddj.pdf

334

Ријешити једначину $2x^2 + 1 = y^2$ у скупу рационалних бројева

Доказ. Пођимо од решења дате једначине (x_1,y_1)=(0,1):
Сва друга решења су дата са $(x, y) = (pt, 1 + qt)$, гдје су p,q цијели и t рационалан. Ако фиксирамо p и q једначина $2x^2 + 1 = y^2$ даје једначину по t: $2p^2t^2 = 2qt + q^2t^2$, одакле је t=0 или $t = \frac{2q}{2p^2-q^2}$. Сада добијамо:

$$x = \frac{2pq}{2p^2-q^2}$$
$$y = \frac{2p^2+q^2}{2p^2-q^2}$$

□

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imomath.com/srb/dodatne/UTB4.pdf

335

Наћи све парове непарних природних бројева a и b мањих од 2^2017 таквих да су бројеви $a^b + b$ и $b^a + a$ дјељиви са 2^{2017}.

Доказ. Пошто је $a^b \equiv a \pmod 4$,из услова задатка следи да $4 \mid a + b$,па можемо да претпоставимо да је $a \equiv 1$ и $b \equiv 3 \pmod 4$. Нека $2^k \mid\mid a - 1$ и $2^l \mid\mid b + 1$, гдје су k,l$\geq$ 2. По леми о дизању експонента имамо $2^{k+1} \mid\mid a^{b-1} - 1$ и $2^{k+l} \mid\mid b^{a-1} - 1$. Следи да $2^{k+1} \mid\mid a(a^{b-1} - 1) - b(b^{ar-1} - 1) = (a^b + b) - (b^a + a)$,одакле је $k \geq 2016$. При томе,a=1 или $a = 2^{2016} + 1$.
Осим тога,пошто је тада $a^b \equiv a \pmod{2^{2017}}$,имамо $2017 \mid a + b$ тј. $b = 2^{2017} - a$
Једина решења (a,b) су парови $(1, 2^{2017} - 1)$ и $(2^{2016} + 1, 2^{2016} - 1)$ са пермутацијама. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imomath.com/srb/dodatne/32zadatka_2017_IMO-pripreme_ddj.pdf

336

Одредити све просте бројеве p и q за које је $p^{q+1} + qp + 1$ потпун квадрат.

Доказ. Једно решење је $p = q = 2$. Претпоставимо да је p непарно и $p^{q+1} + q^{p+1} = x^2$. Тада је $p^{q+1} = (x - q^{\frac{p+1}{2}})(x + q^{\frac{p+1}{2}})$.
Ако су оба чиниоца $x \pm q^{\frac{p+1}{2}}$ дјељиви са p,онда $p \mid 2q^{\frac{p+1}{2}}$ па мора бити p=q,али тада је $x^2 = 2p^{p+1}$, што је немогуће.
Једина преостала могућност је $x - q^{\frac{p+1}{2}} = 1$ и $2q^{\frac{p+1}{2}} + 1 = x + q^{\frac{p+1}{2}} = p^{q+1}$. И ово је немогуће за непарно q јер тада $p^{q+1} \equiv 1$ и $2q^{\frac{p+1}{2}} + 1 \equiv \pmod 4$.
Следи да је q=2. Тада добијамо $2^{\frac{p+3}{2}} = p^3 - 1 = (p - 1)(p^2 + p + 1)$
Међутим,$p^2 + p + 1$ је увијек непарно и веће од 1, што је контрадикција. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
https://imomath.com/srb/dodatne/32zadatka_2017_IMO-pripreme_ddj.pdf

337

Природни бројеви n,m,k су такви да бројеви $5^n - 2$ и $2^k - 5$ дјељиви са $5^m - 2^m$. Доказати да су n и m узајамно прости.

Доказ. Означимо $M = 5^m - 2^m$. Имамо $5^{nk} \equiv 2^k \equiv 5 \pmod{M}$, тј. $M \mid 5^{nk-1} - 1$;аналогно важи $M \mid 2^{nk-1} - 1$,па $M = 5^m - 2^m \mid 5^{nk-1} - 2^{nk-1}$. Одавде слиједи да $m \mid nk - 1$, па је $(m, n) = 1$

Napomena:Позната је чињеница $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$ за a,b$\in \mathbb{Z}$, $(a, b) = 1$ и m,n$\in \mathbb{N}$ □

(**Николина Јеловац 13/18 Д**) задатак преузет са
`https://imomath.com/srb/dodatne/32zadatka_2014_Avala_ddj.pdf`

338

Дат је природан број n. Цио број $a > n^2$ је такав да се међу бројевима $+1, +2, ..., +n$ налази садржалац сваког од бројева $n^2+1, n^2+2, ..., n^2+n$. Доказати да је $a > n^4 - n^3$

Доказ. Нека је $a_i(n^2 + i)$ садржалац броја $n^2 + i$ међу бројевима $+1, ..., +n$. Због $a > n^2$ је $a_1 \geq 1$. Примјетимо да не може да важи $a_1 \leq a_2 \leq \cdots \leq a_n$,у супротном би било $n-1 \geq a_n(n^2+n) - a_1(n^2+1) \geq a_1(n-1)$,што је немогуће. Зато је $a_i > a_{i+1}$ за неко i,а тада је $n-1 \geq a_i(n^2+i) - a_{i+1}(n^2+i+1) \geq a_i(n^2+i) - (a_i-1)(n^2+i+1) = n^2+i+1-a_i$,дакле $a_i \geq n^2 - n + 3$. То значи да је $a + n \geq (n^2 - n + 3)(n^2 + i) > n^2(n^2 - n + 3)$,одакле слиједи $a > n^4 - n^3$. □

(**Николина Јеловац 13/18 Д**) задатак преузет са
`https://imomath.com/srb/dodatne/32zadatka_2013_Avala_ddj.pdf`

339

Ријешти систем конгруенција:

$$x \equiv 0 \pmod{2}$$

$$x \equiv 0 \pmod{3}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 6 \pmod{7}$$

Доказ. Како су 2, 3, 5 и 7 прости бројеви они су такође и међусобно узајамно прости, па на основу **Кинеске теореме о остацима** овај систем има рјешење.
Нека је m производ $m = 2 \cdot 3 \cdot 5 \cdot 7$, односно $m = 210$.
Сада формирамо нови систем конгруенција са остатком 1. Означимо са m_j редом 2, 3, 5 и 7 и са n_j производе свих вриједности m_i осим када је $i = j$. Тада добијамо сљедећи систем:

$$n_1 x_1 \equiv 1 \pmod{m)_1}$$

$$n_2 x_2 \equiv 1 \pmod{m)_2}$$

$$n_3 x_3 \equiv 1 \pmod{m}_3$$
$$n_4 x_4 \equiv 1 \pmod{m}_4$$

Како n_j можемо да изразимо преко m, тада је:

$$(m_2 \cdot m_3 \cdot m_4) \cdot x_1 \equiv 1 \pmod{m}_1$$
$$(m_1 \cdot m_3 \cdot m_4) \cdot x_2 \equiv 1 \pmod{m}_2$$
$$(m_1 \cdot m_2 \cdot m_4) \cdot x_3 \equiv 1 \pmod{m}_3$$
$$(m_1 \cdot m_2 \cdot m_3) \cdot x_4 \equiv 1 \pmod{m}_4$$

Замијенимо промјењиве одговарајућим вриједностима:

$$(3 \cdot 5 \cdot 7) \cdot x_1 \equiv 1 \pmod{2}$$
$$(2 \cdot 5 \cdot 7) \cdot x_2 \equiv 1 \pmod{3}$$
$$(2 \cdot 3 \cdot 7) \cdot x_3 \equiv 1 \pmod{5}$$
$$(2 \cdot 3 \cdot 5) \cdot x_4 \equiv 1 \pmod{7}$$

Па је то даље:

$$105 x_1 \equiv 1 \pmod{2}$$
$$70 x_2 \equiv 1 \pmod{3}$$
$$42 x_3 \equiv 1 \pmod{5}$$
$$30 x_4 \equiv 1 \pmod{7}$$

Прво скратимо добијене вриједности по одговрајућем модулу, па имамо:

$$1 x_1 \equiv 1 \pmod{2}$$
$$1 x_2 \equiv 1 \pmod{3}$$
$$2 x_3 \equiv 1 \pmod{5}$$
$$2 x_4 \equiv 1 \pmod{7}$$

Сада за сваку конгрунецију тражимо одговарајућу вриједност за x_j за коју ће дата конгуренција бити тачна. Крећемо од броја 1 па идемо редом док не нађемо тачан број.Тако добијамо сљедеће:

$$1 \cdot 1 = 1 \equiv 1 \pmod{2}$$
$$1 \cdot 1 = 1 \equiv 1 \pmod{3}$$
$$2 \cdot 3 = 6 \equiv 1 \pmod{5}$$
$$2 \cdot 4 = 8 \equiv 1 \pmod{7}$$

Односно, добили смо сљедеће:

$$x_1 = 1$$
$$x_2 = 1$$
$$x_3 = 3$$

$$x_4 = 4$$

Сада помножимо добијена рјешења са одговарајућим вриједностима n_j и одговарајућим остацима из почетног система и све то саберимо да бисмо нашли рјешење за x_0:

$$x_0 = 1 \cdot 105 \cdot 0 + 1 \cdot 70 \cdot 0 + 3 \cdot 42 \cdot 1 + 4 \cdot 30 \cdot 6 =$$

$$= 0 + 0 + 126 + 720 = 846$$

Сада имамо главну конгруенцију у сљедећем облику:

$$x \equiv x_0 \pmod{m}$$

, а то је:

$$x \equiv 846 \pmod{2)10}$$

$$x \equiv 6 \pmod{2)10}$$

Дакле, наше рјешење је $x = \mathbf{6}$.

То можемо да провјеримо тако што ћемо наше рјешење убацити у почетне једначине, па имамо:

$$6 \equiv 0 \pmod{2} \implies T$$

$$6 \equiv 0 \pmod{3} \implies T$$

$$6 \equiv 1 \pmod{5} \implies T$$

$$6 \equiv 6 \pmod{7} \implies T$$

Ово доказује да је наше рјешење тачно.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://math.dartmouth.edu/~jvoight/Sp2009-255/255-HW05.pdf`

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

340

а) Нека су $a_1, a_2, \ldots, a_n, n \in N$ различити узајамно прости у паровима природни бројеви. Доказати да постоји бесконачно много природних бројева b таквих да су $b + a_1, b + a_2, \ldots, b + a_n$ такође узајамно прости у паровима.

б) Дато је n различитих природних бројева $a_1, a_2, \ldots, a_n$. За сваки прост број p означимо са $r_i(p)$ остатак који се добија при дијељењу броја $a_i, i = 1, 2, \ldots, n$ са p. Доказати и да постоји бесконачно много цијелих бројева b таквих да су $b + a_1, b + a_2, \ldots, b + a_n$ узајамно прости у паровима ако важи следећи услов: За сваки прост број p бар један елемент скупа $\{0, 1, \ldots, p-1\}$ се не појављује више од једног пута међу остацима $r_1(p), r_2(p), \ldots, r_n(p)$.

Доказ. а) Нека је:

$$P = \prod_{i,j=1, i\neq j}^{n} |a_i - a_j|$$

Посматрајмо бесконачни скуп $\{P, 2P, 3P, \ldots\}$. Покажимо да су бројеви $a_1+kP, a_2+kP, \ldots, a_n+kP$ узајамно прости у паровима за сваки природни број k. Претпоставимо супротно. Тада за неке $i, j \in \{1, 2, \ldots, n\}, i \neq j$, бројеви $a_i + kP$ и $a_j + kP$ имају заједнички дјелилац $d > 1$. Из тога произлази да је $a_i - a_j = (a_i + kP) - (a_j + kP)$ дјељиво са d, тј. да је P дјељиво са d. Међутим, ако су и $a_i + kP$ и P дјељиви са d тада $d \mid a_i$. Слично, ако $d \mid a_j + kP$ и $d \mid P$, онда $d \mid a_j$. Дакле, $d > 1$ је заједнички дјелилац бројева a_i и $_j$ супротно претпоставци да су ови бројеви узајамно прости. Дакле, за свако $k \in N$ бројеви $a_i + kP, i = 1, 2, \ldots, n$, су узајамно прости у паровима.

б) Означимо са d разлику између највећег и најмањег од бројева $a_1, a_2, \ldots, a_n$. Претпоставимо да је задати услов испуњен. Посматрајмо све просте бројеве $p \leq d$. За сваки такав p нека је r_p елемент скупа $\{0, 1, \ldots, p-1\}$ који се појављује не више од једном између бројева $r_1(p), r_2(p), \ldots, r_n(p)$. Нека је:

$$r_p^* = \begin{cases} p - r_p, & r_p > 0. \\ 0, & r_p = 0. \end{cases}$$

Пошто су различити прости бројеви узајамно прости, према Кинеској теореми о остацима слиједи да постоји цели број b такав да су конгруенције:

$$b \equiv r_p^* \pmod{p}$$

задовољене за све просте бројеве $p \leq d$.

Докажимо да су бројеви $a_1 + b, a_2 + b, \ldots, a_n + b$ узајамно прости у паровима. Претпоставимо да $a_i + b$ и $a_j + b$ имају заједнички прост фактор $\bar{p}$, за неке $i, j \in \{1, 2, \ldots, n\}, i \neq j$. Разликујемо следеће случајеве:

(1) $\bar{p} > d$. У овом случају из

$$a_i + d \equiv 0 \pmod{\bar{p}} \text{ и } a_j + b \equiv 0 \pmod{\bar{p}}$$

слиједи да $p \mid a_i - a_j$, тј. да је $|a_i - a_j| \geq \bar{p}$, што је у контрадикцији са $\bar{p} > d \geq |a_i - a_j|$.

(2) $\bar{p} \leq d$. У овом случају имамо да је:

$$a_i + b = (mp + r_i(p)) + (np + r_p^*) \text{ и } a_j + b = (lp + r_j(p)) + (np + r_p^*)$$

гдје су m, n, l неки цијели бројеви.

Претпоставимо да је $r_p^* = p - r_p$. Тада је број $a_i + b$ дјељив са p само ако је $r_i(p) - r_p$ дјељив са p, тј. ако је $r_i(p) = r_p$. Слично томе, $a_j + b$ је дјељиво је са p ако је $r_j(p) = r_p$. Међутим, остатак r_p појављује се највише једном у скупу остатака $\{r_1(p), r_2(p), \ldots, r_n(p)\}$ што је контрадикција.

Ако је $r_p^* = 0$, тада су оба броја $r_i(p)$ и $r_j(p)$ дељиви са p. Ово доводи до једнакости $r_i(p) = r_j(p) = 0 = r_p$, што нас враћа до контрадикције са избором броја r_p.

Тако су бројеви $a_1 + b, a_2 + b, \ldots, a_n + b$ узајамно прости у паровима. Нека је:

$$P^* = \prod_{i,j=1, i \neq j}^{n} | (a_i + b) - (a_j + b) |$$

Према доказу из задатка а) бројеви:

$$a_1 + b + kP^*, a_2 + b + kP^*, \ldots, a_n + b + kP^*$$

су узајамно прости у паровима. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

341

Наћи последње двије цифре броја $7^{7^{1000}}$.

Доказ. Примијетимо да је

$$\phi(100) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = 40$$

По Ојлеровој теореми је $7^{40} \equiv 1 \pmod{100}$.

Сада имамо да је $\phi(40) = \phi(2^3)\phi(5) = 4 \cdot 4 = 16$, а самим тим $7^{16} \equiv 1 \pmod{40}$.

Како је $1000 = 16 \cdot 62 + 8$, имамо да је $7^{1000} \equiv (7^{16})^{62}7^8 \equiv 1^{62}7^8 \equiv (7^4)^2 \equiv 1^2 \equiv 1 \pmod{40}$. Из тога слиједи да је $7^{1000} = 1 + 40t$ za neki cijeli broj t. Спојимо све у једно и добијамо:

$$7^{7^{1000}} \equiv 7^{1+40t} \equiv 7 \cdot (7^{40})^t \equiv 7 \pmod{100}$$

Овим смо добили да су последње двије цифре 07. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=6024B41025E64542A29E9485D93358EA?doi=10.1.1.649.6499&rep=rep1&type=pdf`

342

5 рубина, 8 сафире, 7 бисера и 92 новчића вриједе исто као и 19 рубина, 14 сафира, 2 бисера и 4 новчића. Колико новчића вриједе рубини, сафири и бисери појединачно?

Доказ. Нека r, s и p буду вриједности рубина, сафира и бисера.

Тада имамо да је $5r + 8s + 7p + 92 = 19r + 14s + 2p + 4$ из чега добијамо $14r + 6s - 5p = 88$.

Почнимо са двије непознате тј. са $14r + 6s$. НЗД$(14, 6) = 2$ па то записујемо као $14(1) + 6(-2) = 2$. То значи да вриједност рубина и сафира мора бити дјељива са 2, тј. можемо их записивати као $2n$ за неко n.

Након тога обратимо пажњу на $2n - 5p = 88$. НЗД$(2, 5) = 1$ па записујемо као $2(3) - 5(1) = 1$. Помножимо све са 88 и добијамо $2(264) - 5(88) = 88$. Дакле свако рјешење $2n - 5p = 88$ се може записати као:

$$n = 264 - 5t$$
$$p = 88 - 2t$$

за свако $t \in Z$.

Вратимо се у $14(1) + 6(-2) = 2$ и помножимо све са $n = 264 - 5t$. Добијамо $14(264 - 5t) + 6(-528 + 10t) = 2(264 - 5t)$. Дакле свако рјешење $14r + 6s - 5p = 88$ мора бити записано као:

$$r = 264 - 5t + 3u$$
$$s = -528 + 10t - 7u$$
$$p = 88 - 2t$$

за свако $t, u \in Z$. Тражимо позитивне цијеле бројеве па знамо да је $88 - 2t > 0$ тј. $t < 44$.

Из овога и из једначине за s, добијамоо да је $u < -14$. С обзиром да је $t = 43 - x$ и $u = -14 - y$ добијамо да је:

$$\begin{aligned} r &= 264 - 5t + 3u \\ s &= -528 + 10t - 7u \\ p &= 88 - 2t \end{aligned}$$

за неко $x, y \geq 0$.

На примјер, из $x = y = 0$ слиједи да је $r = 4, s = 7$ и $p = 2$, док за $x = y = 1$ добијамо да је $r = 6, r = 4, p = 4$. Иако не важи за свако, постоји бесконачно много вриједности x и y из којег се добија позитивно рјешење. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://web.math.ucsb.edu/~agboola/teaching/2005/winter/old-115A/sol3.pdf`

343

Користећи Ојлерови теорему доказати:

а) За сваки природан број a важи $a^{37} \equiv a \pmod{1729}$.

б) За сваки природан број a важи $a^{33} \equiv a \pmod{4080}$.

Доказ. а) Претпоставимо да је НЗД$(a, 1729) = 1$, гдје је $1729 = 7{\cdot}13{\cdot}19$. Онда је НЗД$(a, 19) = 1$ а онда је $a^{\phi(19)} \equiv 1 \pmod{19}$ тј. $a^{18} \equiv 1 \pmod{19}$. Из овога слиједи да је $a^{36} \equiv 1 \pmod{19}$.

Такође, НЗД$(a, 13) = 1$ а онда је $a^{\phi(13)} \equiv 1 \pmod{13}$ тј. $a^{12} \equiv 1 \pmod{13}$. Одатле видимо да је $a^{36} \equiv 1 \pmod{13}$.

Коначно, из НЗД$(a, 7) = 1$ слиједи да је $a^{\phi(7)} \equiv 1 \pmod{7}$ или $a^6 \pmod{7}$. Самим тим је $a^{36} \equiv 1 \pmod{7}$.

Сада слиједи да је $a^{37} \equiv a \pmod{7}, a^{37} \equiv a \pmod{13}$ и $a^{37} \equiv a \pmod{19}$. Даље, свака од ових конгруенција исто важи и ако $7 \mid a, 13 \mid a$ или $19 \mid a$. Дакле закључујемо да је

$$a^{37} \equiv a \pmod{7 \cdot 13 \cdot 19}$$

за свако a.

б) Претпоставимо да је a непарни цијели број такав да НЗД$(a, 4080) = 1$. Имамо да је $4080 = 15 \cdot 16 \cdot 17$.

Из Ојлерове теореме, као и тога да је $\phi(15) = 8, \phi(16) = 8$ и $\phi(17) = 16$, слиједи да је $a^8 \equiv 1 \pmod{15}, a^8 \equiv 1 \pmod{16}$ и $a^{16} \equiv 1 \pmod{16}$, а $a^{32} \equiv 1 \pmod{17}$.

Одатле слиједи да је $a^{33} \equiv a \pmod{15}, a^{33} \equiv 1 \pmod{16}$ и $a^{33} \equiv 1 \pmod{17}$. Даље, свака од тих конгруенција важи за било које непарно a. Одатле добијамо да

$$a^{33} \equiv a \pmod{15 \cdot 16 \cdot 17}$$

за било које непарно a. □

(**Лука Брацовић 17/17 Д**) задатак преузет са:
`http://web.math.ucsb.edu/~agboola/teaching/2005/winter/old-115A/sol3.pdf`

344

Користећи Малу Фермаову теорему доказати да ако је p непаран прост број, онда:

а) $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$

б) $1^{p} + 2^{p} + 3^{p} + \cdots + (p-1)^{p} \equiv 0 \pmod{p}$

Доказ. Како је НЗД$(a, p) = 1$ за све природне бројеве $1 \leq a \leq p-1$, из Мале Фермаове теореме слиједи да је $a^{p-1} \equiv 1$ за свако a.

а) По модулу p имамо да је

$$1^{p-1} + \cdots + (p-1)^{p-1} \equiv 1 + \cdots + 1 \pmod{p} \equiv p - 1 \pmod{p} \equiv -1 \pmod{p}$$

б) Као и у претходном задатку, по модулу p имамо

$$1^{p} + 2^{p} + \cdots + (p-1)^{p} \equiv 1 + 2 + \cdots + p - 1 \pmod{p} \equiv \frac{(p-1)p}{2} \pmod{p} \equiv 0 \pmod{p}$$

□

345

Ријешити древни индијски проблем који гласи: "Ако из корпе уклањамо по 2 јајета истовремено, на крају ће их у корпи остати 1. Ако уклањамо по 3, 4, 5 или 6 јаја истовремено, тада ће у корпи остајајти редом 2, 3, 4 или 5. Ако уклањамо по 7, на крају неће остати ни једно јаје у корпи. Који је најмањи могући број јаја у корпи?"

Доказ. Овај задатак можемо поставити у облику система конгруенција који даље рјешавамо, па имамо:

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod 4$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 0 \pmod 7$$

Видимо да бројеви 2, 4 и 6 нијесу узајамно прости, па да бисмо могли да користимо *Кинеску теорему о остацима* морамо ово да ријешимо.
Примијетимо да конгруенцију $x \equiv 5 \pmod 6$ можемо да раставимо на на двије конгрунеције по модулу 2 и 3, односно: $x \equiv 5 \pmod 2$ и $x \equiv 5 \pmod 3$, при чему је $x \equiv 5 \pmod 2 \implies x \equiv 1 \pmod 2$ и $x \equiv 5 \pmod 3 \implies x \equiv 2 \pmod 3$. Због тога ћемо пету конгруенцију да занемаримо. Остаје нам проблем са 2 и 4. Занемаримо и конгруенцију по модулу 2 за сада. Ово значи да имамо 4 конгруенције, и то:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 4$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 0 \pmod 7$$

Нека је m производ $m = 3 \cdot 4 \cdot 5 \cdot 7$, односно $m = 420$. Сада формирамо нови систем конгруенција са остатком 1. Означимо са m_j редом 3, 4, 5 и 7 и са n_j производе свих вриједности m_i осим када је $i = j$. Тада добијамо сљедећи систем:

$$n_1 x_1 \equiv 1 \pmod m_1$$
$$n_2 x_2 \equiv 1 \pmod m_2$$
$$n_3 x_3 \equiv 1 \pmod m_3$$
$$n_4 x_4 \equiv 1 \pmod m_4$$

Како n_j можемо да изразимо преко m, тада је:

$$(m_2 \cdot m_3 \cdot m_4) \cdot x_1 \equiv 1 \pmod m_1$$
$$(m_1 \cdot m_3 \cdot m_4) \cdot x_2 \equiv 1 \pmod m_2$$
$$(m_1 \cdot m_2 \cdot m_4) \cdot x_3 \equiv 1 \pmod m_3$$
$$(m_1 \cdot m_2 \cdot m_3) \cdot x_4 \equiv 1 \pmod m_4$$

Замијенимо промјењиве одговарајућим вриједностима:

$$(4 \cdot 5 \cdot 7) \cdot x_1 \equiv 1 \pmod 3$$
$$(3 \cdot 5 \cdot 7) \cdot x_2 \equiv 1 \pmod 4$$
$$(3 \cdot 4 \cdot 7) \cdot x_3 \equiv 1 \pmod 5$$
$$(3 \cdot 4 \cdot 5) \cdot x_4 \equiv 1 \pmod 7$$

Па је то даље:

$$140 x_1 \equiv 1 \pmod 3$$

$$105x_2 \equiv 1 \pmod 4$$
$$84x_3 \equiv 1 \pmod 5$$
$$60x_4 \equiv 1 \pmod 7$$

Прво скратимо добијене вриједности по одговрајућем модулу, па имамо:

$$2x_1 \equiv 1 \pmod 3$$
$$1x_2 \equiv 1 \pmod 3$$
$$4x_3 \equiv 1 \pmod 5$$
$$4x_3 \equiv 1 \pmod 7$$

Сада за сваку конгрунецију тражимо одговарајућу вриједност за x_j за коју ће дата конгуренција бити тачна. Крећемо од броја 1 па идемо редом док не нађемо тачан број.Тако добијамо сљедеће:

$$2 \cdot 2 = 4 \equiv 1 \pmod 3$$
$$1 \cdot 1 = 1 \equiv 1 \pmod 4$$
$$4 \cdot 4 = 16 \equiv 1 \pmod 5$$
$$4 \cdot 2 = 8 \equiv 1 \pmod 7$$

Односно, добили смо сљедеће:

$$x_1 = 2$$
$$x_2 = 1$$
$$x_3 = 4$$
$$x_4 = 2$$

Сада помножимо добијена рјешења са одговарајућим вриједностима n_j и одговарајућим остацима из почетног система и све то саберимо да бисмо нашли рјешење за x_0:

$$x_0 = 2 \cdot 140 \cdot 2 + 1 \cdot 105 \cdot 3 + 4 \cdot 84 \cdot 4 + 2 \cdot 60 \cdot 0 =$$
$$= 560 + 315 + 1344 + 0 = 2219$$

Сада имамо главну конгруенцију у сљдећем облику:

$$x \equiv x_0 \pmod m$$

, а то је:

$$x \equiv 2219 \pmod 4 20$$
$$x \equiv 119 \pmod 4 20$$

Дакле, наше рјешење је $x = \mathbf{119}$.

То можемо да провјеримо тако што ћемо наше рјешење убацити у почетне једначине, па имамо:

$$119 \equiv 1 \pmod 2 \implies T$$
$$119 \equiv 2 \pmod 3 \implies T$$

$$119 \equiv 3 \pmod 4 \implies T$$
$$119 \equiv 4 \pmod 5 \implies T$$
$$119 \equiv 5 \pmod 6 \implies T$$
$$119 \equiv 0 \pmod 7 \implies T$$

Ово доказује да је наше рјешење тачно. Па можемо рећи да је најмањи могући број јаја у корпи **119**.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://math.dartmouth.edu/~jvoight/Sp2009-255/255-HW05.pdf`

346

Ријешити конгруенцију: $x^2 + 2x - 1 \equiv 0 \pmod 7$.

Доказ. Како је број 7 прост број, ово може да се ријеши на лакши начин.
Да бисмо ријешили ову конгруенцију, прво морамо да средимо њен квадратни дио. То ћемо да урадимо тако што ћемо да искористимо *формулу за квадрат збира* на сљедећи начин:

$$x^2 + 2x - 1 \equiv 0 \pmod 7 \implies x^2 + 2x \equiv 1 \pmod 7 \implies$$
$$x^2 + 2x + 1 \equiv 1 + 1 \pmod 7 \implies (x+1)^2 \equiv 2 \pmod 7$$

Сада не можемо ништа да урадимо са 2, јер у конгруенцији радимо само са цијелим бројевима, али како је то конгруенција, на 2 можемо да додајемо 7 све док не добијемо неки одговарајући број, у овом случају нам треба квадрат неког броја, па имамо број 9 као квадрат броја 3, па је:

$$(x+1)^2 \equiv 2 \pmod 7 \implies (x+1)^2 \equiv 9 \pmod 7 \implies x + 1 \equiv +/- 3 \pmod 7$$

Па из овога имамо два рјешења:
1) $x + 1 \equiv 3 \pmod 7 \implies x \equiv 2 \pmod 7$
2) $x + 1 \equiv -3 \pmod 7 \implies x \equiv -4 \pmod 7 \implies x \equiv 3 \pmod 7$
Ово значи да су рјешења наше конгруенције бројеви **2** и **3**.
Ако испробамо ове вриједности у конгруенцији, добијамо тачан резултат.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://math.dartmouth.edu/~jvoight/Sp2009-255/255-HW05.pdf`

347

Ријешити конгруенцију: $x^2 \equiv 26 \pmod{55}$.

Доказ. Како број 55 није прост, ово мора да се рјешава на тежи начин - уз помоћ **Кинеске теореме о остацима**.
Број 5 може да се растави на просте чиниоце 5 и 11, односно: $55 = 5 \cdot 11$, па на основу тога од нашу конгруенцију можемо да раставимо на двије нове: $x^2 \equiv 26 \pmod 5$ і $x^2 \equiv 26 \pmod{11}$. Нађимо рјешења за њих.

$$x^2 \equiv 26 \pmod 5 \implies x^2 \equiv 1 \pmod 5$$

Из овога имамо два рјешења: $x \equiv 1 \pmod 5$ і $x \equiv -1 \pmod 5 \implies x \equiv 4 \pmod 5$

$$x^2 \equiv 26 \pmod{11} \implies x^2 \equiv 4 \pmod{11}$$

Из овога такође имамо два рјешења: $x \equiv 2 \pmod{11}$ и $x \equiv -2 \pmod 1 1 \implies x \equiv 9 \pmod{11}$.
Сада имамо 4 рјешења и њих комбинујемо у системе од по двије једначине по принципу *свако са сваким*, па тако добијамо 4 система која ћемо да рјешавамо.

$$x \equiv 1 \pmod 5$$
$$x \equiv 2 \pmod{11}$$

Из прве једначине видимо да је $x = 1 + 5k$, па то замијенимо у другој и добијамо:

$$1 + 5k \equiv 2 \pmod{11} \implies 5k \equiv 1 \pmod{11}$$

Желимо да се ријешимо броја 5, па ћемо да помножимо све са неким бројем који ће нам омогућити да умјесто 5 добијемо 1. То је број 9.

$$9 \cdot 5k \equiv 9 \cdot 1 \pmod 1 1 \implies 45k \equiv 9 \pmod{11} \implies$$

$$k \equiv 9 \pmod{11}$$

Па можемо да запишемо сљедеће: $k = 9 + 11l$. Сада се вратимо у прву једначину и замијенимо ово: $x = 1 + 5(9 + 11l) = 46 + 55l$. То сада вратимо натраг у конгруенцију, па имамо:

$$x \equiv 46 \pmod{55}$$

Урадимо исто ово и за друге случајеве.

$$x \equiv 1 \pmod 5$$
$$x \equiv 9 \pmod{11}$$

И овдје добијамо сљедеће:

$$x \equiv 31 \pmod{55}$$

$$x \equiv 4 \pmod 5$$
$$x \equiv 2 \pmod{11}$$

И овдје добијамо сљедеће:

$$x \equiv 24 \pmod{55}$$

$$x \equiv 4 \pmod{5}$$
$$x \equiv 9 \pmod{11}$$

И овдје добијамо сљедеће:

$$x \equiv 9 \pmod{55}$$

Као што видимо, за рјешење ове једначине смо добили 4 рјешења, и то:

$$x \equiv 46 \pmod{55}$$
$$x \equiv 31 \pmod{55}$$
$$x \equiv 24 \pmod{55}$$
$$x \equiv 9 \pmod{55}$$

, односно:

$$x = 46$$
$$x = 31$$
$$x = 24$$
$$x = 9$$

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://www.youtube.com/watch?v=azGV8megnXY`

348

За **линеарну диофантову једначину** $17x + 13y = 100$ наћи рјешење или показати да нема рјешње.

Доказ. Да бисмо провјерили да ли наша једначина има рјешење, прво нађемо најмањи заједнички дјелилац за бројеве уз x и x, односно нзд$(17, 13)$ =?. Иако знамо да су ово прости бројеви и да је за њих заједнички дјелилац 1, ми иначе за ово можемо користити *Еуклидов алгоритам*:

$$17 = 13 \cdot 1 + 4$$
$$13 = 4 \cdot 3 + 1$$
$$4 = 1 \cdot 4 + 0$$

Када смо добили да је остатак 0, вратимо се један корак назад и узмемо тај остатак, па можемо рећи да је нзд$(17, 13) = 1$. Сада провјеравамо да ли 1 дијели број 100, што је тачно,

па закључујемо да наша једначина има рјешење.
Како смо нашли нзд$(17, 13)$, сада можемо да запишемо једначине за тражена рјешења:

$$x = \frac{100}{1} \cdot x_0 + \frac{13}{1} \cdot t, t \in Z$$

$$y = \frac{100}{1} \cdot y_0 + \frac{17}{1} \cdot t, t \in Z$$

Требају нам само још вриједности за x_0 и y_0. Њих одређујемо из претходног поступка са Еуклидовим алгоритмом тако што кренемо од броја који смо раније узели за најмањи заједнички дјелилац и идемо у супротном смјеру у односу на ток алгоритма. Уз то срећујемо израз, али чувамо вриједности које се налазе уз x и y у једначини. Па имамо:

$$1 = 13 - 4 \cdot 3 = 13 - (17 - 13 \cdot 1) \cdot 3 =$$

$$= 13 - 17 \cdot 3 + 13 \cdot 3 = 13 \cdot (1 + 3) - 17 \cdot 3 =$$

$$= 13 \cdot 4 - 17 \cdot 3 = y \cdot 4 - x \cdot 3$$

Као што видимо, уз x имамо број -3, а уз y је број 4, па су то наше тражене вриједности:

$$x_0 = -3$$

$$y_0 = 4$$

Сада ове вриједности уврстимо у једначине за x и y и то средимо:

$$x = 100 \cdot (-3) + 13 \cdot t, t \in Z$$

$$y = 100 \cdot 4 + 17 \cdot t, t \in Z$$

Рјешења наше једначине су:

$$x = -300 + 13t, t \in Z$$

$$y = 400 + 17t, t \in Z$$

Сада можемо да провјеримо да ли су наша рјешења тачна. Узмимо да је $t = 0$, тада имамо:

$$x = -300 + 13 \cdot 0 = -300$$

$$y = 400 + 17 \cdot 0 = 400$$

Замијенимо то у једначини и добијамо:

$$17 \cdot (-300) + 13 \cdot 400 = 100$$

$$-5100 + 5200 = 100$$

$$100 = 100 \implies T$$

Овим смо доказали да је наше рјешење тачно.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://math.dartmouth.edu/~jvoight/Sp2009-255/255-HW04.pdf`

349

Да ли је могуће да имамо 50 новчића који могу бити од 1, 10 или 25 центи, а да њихова укупна сума буде 3$?

Доказ. Означимо са x број новчића од 1 цента, са y број новчића од 10 центи и са z број новчића од 25 центи. Укупно имамо 50 новчића, па је:

$$x + y + z = 50$$

Када узмемо у обзир колико врједи који новчић и колико центи има у 3$, па имамо:

$$x + 10y + 25z = 300$$

Из прве једначине изразимо x и замијенимо га у другој једначини:

$$x = 50 - y - z$$

$$50 - y - z + 10y + 25z = 300$$

$$9y + 24z = 250$$

Видимо да смо добили *линеарну диофантову једначину* коју даље рјешавамо.
Нађемо прво нзд$(9, 24) =?$ уз помоћ *Еуклидовог алгоритма*:

$$24 = 9 \cdot 2 + 6$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2 + 0$$

Видимо да је

$$\text{нзд}(9, 24) = 3$$

Сад провјеравамо да ли 3 дијели 250. Видимо да је $250 = 3 \cdot 83 + 1$,а то значи да

$$3 \nmid 250$$

, па ова диофантова једначина нема рјешење.

Из овога слиједи да није могуће да имамо ситуацију која задовољава услове нашег задатка.

□

(**Ахмедин Муратовић 22/17 Д**) задатак преузет са:
`https://math.dartmouth.edu/~jvoight/Sp2009-255/255-HW04.pdf`

350

Доказати да ако D било који број различит од 0 онда једначина $x^2 - Dy^2 = z^2$ има бесконачно много ријечења међу позитивним цијлим бројевима x, y, z таквим да $(x, y) = 1$

Доказ. Ако је D непарно онда ке sa цијели број $k > 1$ број $D + 2^{2k-2}$ непаран, па имамо $(D + 2^{2k-2}, 2^k)$, из тога произилази да

$$(D + 2^{2k-2})^2 - D(2^k)^2 = (D - 2^{2k-2})^2 \tag{4.11}$$

. можемо узети да је $x = |D+2^{2k-2}, y = 2^k, z = |D-2^{2k-2}|$. Ако је D парно, онда је за сваки број $y > 1$: $(\frac{1}{2}Dy^2 + 1, y)$ и

$$(\frac{1}{2}Dy^2 + 1)^2 - Dy^2 = (\frac{1}{2}Dy^2 - 1)^2$$

па закључујемо да је

$$x = |\frac{1}{2}Dy^2 + 1|, z = |\frac{1}{2}Dy^2 - 1|$$

.

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

351

Доказати да једначина $xy + x + y = 2^{32}$ има ријешење у позитивним цијелим бројевима и да постоји само једно ријешење када је $x \leq y$

Доказ. Ова једначина је иста као и једначина $2^{2^5} + 1 = (x+1)(y+1)$. Пошто је $F_5 = 2^{2^5} + 1$ Фермаов број (Фермаови бројеви су специјална група бројева који се генеришу формулом $F_n = 2^{2^n} + 1$) једнако производу два парна броја од којих је мањи 641 имамо само једно ријешење у овој једначини а то је x и $y \geq x$ гдје је $x = 640$

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

352

Доказати да једначина $x^2 - 2y^2 + 8z = 3$ нема ријешење међу позитивним бројевима x, y, z

Доказ. Ако је y парно, онда једначина

$$x^2 = 3 - 8z + 2y^2$$

даје остатак 3 при дијељењу са 8 што није могуће. Ако је y непарно онда је $y = 2k + 1$ гдје је k цијели број, па је $x^2 = 3 - 8z + 8k^2 + 2$ што даје остатак 5 при дијељењу са 8 што је такође немогуће јер квадрат сваког непарног броја даје остатак 1 при дијељењу са 8.

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf

353

Пронаћи сва рационална ријешења једначине

$$x^2 + y^2 + z^2 + x + y + z = 1$$

Доказ. Једначина

$$x^2 + y^2 + z^2 + x + y + z = 1$$

нема рационалних ријешења јер је лако видљиво да је еквивалентна једначини

$$(2x+1)^2 + (2y+1)^2 + (2z+1)^2 = 7$$

и да би број 7 требао да буде сума три квадрата рационалних бројева. Требамо приказати да је то немогуће. Заправо, ако би 7 био сума три квадрата рационалих бројева, онда би након множења заједничким имениоцем имали:

$$a^2 + b^2 + c^2 = 7m^2$$

гдје су a, b и c позитивни цијели бројеви, и m је позитивни цијели број. Онда, би постојао најмањи позитивни број m за који горња једначина има ријешење у бројевима a, b, c и оно би било парно, пошто су $a = 2a_1, b = 2b_1, c = 2c_1$ гдје су a_1, b_1, c_1 цијели бројеви. Ако би смо ово укључили у горе поменуту једначину добили би смо, с обзиром на то да је $m^2 = 4n^2$:

$${a_1}^2 + {b_1}^2 + {c_1}^2 = 7n^2$$

гдје је n позитивни цијели број $< m$, супротно претпоставци да је m најмањи позитивни цијели број за који је $7m^2$ збир квадрата три цијела броја. Међутим m је непарно и m^2 даје остатак 1 при дијељењу са 8. Међутим десна страна једначине даје остатак 7 при дијељењу са 8 а ми знамо да не постоји број који може бити збир тих квадрата цијелих бројева

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf

354

За сваки природни број m, пронаћи сва ријешења једначине

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = m$$

у релативно простим бројевима x, y, z

Доказ. Наша једначина је еквивалентна једначини $x^2z + y^2 + z^2y = mxyz$ гдје су бројеви x, y, z различити од 0 и релативно прости. Слиједи да $y \mid x^2z, z \mid y^2x$ и $x \mid z^2y$ јер је $(x, y) = 1, (z, y) = 1$ што имплицира да $(x^2z, y) = 1$ које добијамо из $x \mid z^2y$ је $y = \pm 1$. На сличан начин можемо наћи како је $z = \pm 1$ и $x = \pm 1$. Ако су сва три броја x, y, z са истим знаком. онда наша једначина указује да је $1 + 1 + 1 = m$ дакле да је $m = 3$. Ако би два он њих били негативни и један позитиван тада би наше m било негативно што је контрадикторно првобитној претпоставци. Дакле, за позитивно имамо следећу једначину:

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{y} > m$$

, која има цијелобројно рјешење x, y, z гдје су $m = 3$ релативно прости само за $m = 3$ а у овом случају постоје само два рјешења $x = y = z = 1$ и $x = y = z = -1$. За позитиван цијели број различит од 3, једначина нема рјешење у цијелим бројевима x, y, z различитим од 0 који су међусобно релативно прости. □

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

355

Доказати да једначина

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 1$$

нема рјешења за позитивне цијеле бројеве x, y, z

Доказ. Имамо

$$\frac{x}{y} \cdot \frac{y}{z} \cdot \frac{z}{y} = 1$$

, пошто су бројеви рационални и прости, $\frac{x}{y}$, $\frac{y}{z}$, и $\frac{z}{y}$ не може бити < 1 ако је барем један од њих ≥ 1 онда је

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{y} > 1$$

, и лијева страна једначине не може бити 1 за позитивне цијеле бројеве x, y, z.

□

(**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

356

Доказати да је теорема $_1$ која каже да не постоје позитивни цијели бројеви x, yz за које је $x/y + y/z = z/x$ еквивалентна теореми T_2 која каже да не постоје рјешења једначине $u^3 + v^3 = w^3$ у позитивним бројевима u, v, w

Доказ. Претпоставимо да теорема T_1 важи. Ако је теорема T_2 нетачна онда би постојали цијели бројеви u, v и w такви да је $u^3 + v^3 = w^3$ и ако извршимо следећу измјену $x = u^2v, y = v^2w, z = w^2u$, имаћемо

$$\frac{x}{y} + \frac{x}{y} = \frac{u^2v}{v^2w} + \frac{v^2w}{w^2u} = \frac{u^2}{vw} + \frac{v^2}{wu} = \frac{u^3 + v^3}{uvw} = \frac{w^3}{uvw} = \frac{z}{x}$$

супротно теореми T_1. Тако смо показали да теорема T_1 подразумјева теорему T_2 Претпоставимо да је T_1 нетачно. Онда би постојали цијели бројеви x, y, z такви да

$$\frac{x}{y} + \frac{y}{z} = \frac{z}{x}, x^2z + y^2x = z^2y \tag{4.12}$$

Нека је $x^2z = a, y^2x = b$; требало би онда да су $z^2y = a + b$и $ab(a + b) = (xyz)^3$ Нека је $d = (a, b)$, тако да $a = da_1, b = db_1$ гдје је $(a_1, b_1) = 1$. Слиједи да $a + b = d(a_1 + b_1)$ и $a_1b_1(a_1 + b_1)d^3 = (xyz)^3$. То указује да је $d^3 \mid (xyz)^3$ јер је $d \mid xyz$ и $xyz = dt$, гдје је t позитивни цијели број. Дакле, имамо $a_1b_1(a_1 + b_1) = t^3$ и пошто је a_1, b_1 и $a_1 + b_1$ међусобно релативно птосто, слиједи да $a_1 = u^3, b_1 = v^3, a_1 + b_1 = w^3$ гдје су u, v и w позитивни цијели бројеви. Тако да је $u^3 + v^3 = w^3$ супротно теореми T_2 која подразумјева теорему T_1. Закључујемо да су T_1 и T_2 еквивалентни што је и требало доказати. (**Љиљана Госпић 2/17 Д**) задатак преузет са
`https://www.isinj.com/mt-aime/25020Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf` □